Qualys TotalCloud FlexScan Playbook

March 28, 2023

Qualys, Inc.

919 E Hillsdale
Blvd4th Floor

Foster City, CA
944041 (650) 801
6100

Contents

Qualys TotalCloud – Unified Vulnerability, Threat, and Posture Management

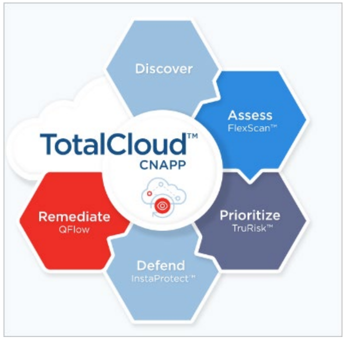
Managing cyber risks across cloud workloads, services, resources, users, and applications is a major challenge as business applications and on-premises infrastructure migrate to the cloud. Cloud applications are especially vulnerable to attacks due to siloed cloud-security tools that increase asset protection costs and complexity.

Frequently asked questions

- I have a new account being added to my cloud eco system, but I am unable to see what is deployed in my account (blind spots).
- I observe certain vulnerable resources being deployed, but I only learn about them after a few hours have passed. How can I gain rapid asset visibility and vulnerabilities?
- I have several cloud services that are deployed using IaC templates, however I occasionally see misconfigurations after deployment that are difficult to correct.
- I have an offline task that I cannot scan till it is operational. After it's started, I notice a slew of discoveries, but it's too late because it may include active exploits.
- I have publicly faced cloud workload, I know it, and require that it be made public. How can I proactively gather an attacker's perspective on vulnerabilities?

How can Qualys help?

Qualys TotalCloud is a cloud-native security product that provides the following benefits:



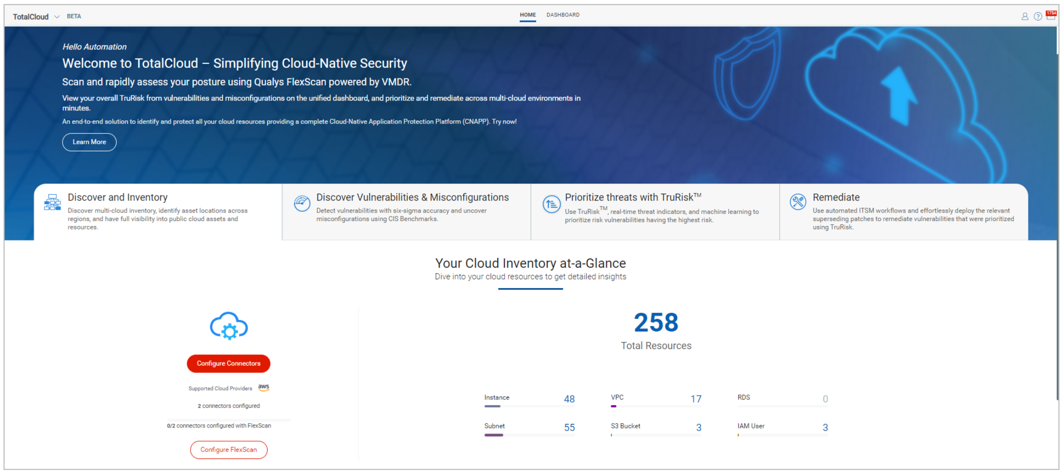
- Offers **maximum security coverage** of your infrastructure through agent and multiple agentless assessment option.
- Provides **highly accurate and trustworthy** detection of vulnerabilities and misconfigurations.
- Consolidates **workload and cloud posture** into a single risk-based metric and provides specific insights to reduce the risk.
- Reduces **risk by automating the remediation** of your highest-risk assets.
- Provides **proactive security** by checking for security issues before deployment.

Read more about FlexScan in our blogs:
Why Is Snapshot Scanning Not Enough?
Use Qualys Flow to Automate Detection & Remediation with No-code Workflows
In-Depth Look Into Data-Driven Science Behind Qualys TruRisk
Introducing TotalCloud – Cloud Security Simplified
Announcing General Availability of Qualys TotalCloud
Real-Time Defense of Multi-Cloud Environments From Malicious Attacks and Threats

Refer Qualys blogs to know more about strengthening your defenses consistent with CISA Shields Up guidelines and Qualys Documentation to set up and configure Qualys apps.

Let's Get Started

Let's look at the Qualys and AWS configurations required to enable Zero-Touch API Scans.



Hello Automation

Welcome to TotalCloud – Simplifying Cloud-Native Security

Scan and rapidly assess your posture using Qualys FlexScan powered by VMDR.

View your overall TruRisk from vulnerabilities and misconfigurations on the unified dashboard, and prioritize and remediate across multi-cloud environments in minutes.

An end-to-end solution to identify and protect all your cloud resources providing a complete Cloud-Native Application Protection Platform (CNAPP). Try now!

Discover and Inventory
Discover multi-cloud inventory, identify asset locations across regions, and have full visibility into public cloud assets and resources.

Discover Vulnerabilities & Misconfigurations
Detect vulnerabilities with six-sigma accuracy and uncover misconfigurations using CIS Benchmarks.

Prioritize threats with TruRisk™
Use TruRisk™, real-time threat indicators, and machine learning to prioritize risk vulnerabilities having the highest risk.

Remediate
Use automated ITSM workflows and effortlessly deploy the relevant superseding patches to remediate vulnerabilities that were prioritized using TruRisk.

Your Cloud Inventory at-a-Glance
Dive into your cloud resources to get detailed insights

Supported Cloud Providers aws

2 connectors configured

0/2 connectors configured with FlexScan

258
Total Resources

Instance	48	VPC	17	RDS	0
Subnet	55	S3 Bucket	3	IAM User	3

Scan and Rapidly Assess Your Posture Using Qualys FlexScan Powered by VMDR

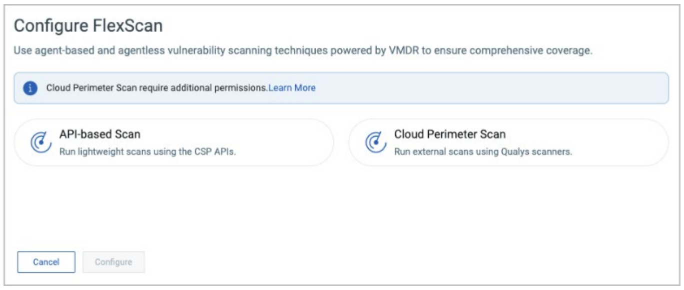
Qualys FlexScan is the new zero-touch, cloud-native method of conducting agent and agentless security assessments. Zero-touch means that no complicated configurations, such as IP ranges, regions, connectors, etc., are required, nor is there a requirement to create a schedule to enable scanning.

How will Qualys TotalCloud with FlexScan simplify cloud security products?

- Automatically uses the cloud APIs.
- Determines the appropriate configuration parameters.
- Starts scanning as soon as it discovers a new workload.
- Leverages Qualys' 6-sigma (Show 99.99966%) accuracy scanning capabilities.
- Reduces false positives so that you can focus on critical vulnerabilities.

Qualys FlexScan Scanning Options

FlexScan supports the following scanning options.



Configure FlexScan

Use agent-based and agentless vulnerability scanning techniques powered by VMDR to ensure comprehensive coverage.

Cloud Perimeter Scan require additional permissions.Learn More

API-based Scan

Run lightweight scans using the CSP APIs.

Cloud Perimeter Scan

Run external scans using Qualys scanners.

API-based Scan

- FlexScan uses Cloud Service Provider (CSP)-provided APIs.
- Gathers operating system (OS) package inventory for vulnerability analysis.
- API-based assessment is quick.
- Best suited for short-lived workloads and the initial assessment of new workloads.

Network-based Scan

- FlexScan can use network scanner appliances to assess workloads over the network.
- Automatically instantiate the network scanning of the workload in the appropriate network.
- Network scanners provide similar assessment capabilities as an agent.
- Networks should be used to assess workloads facing the internet and for workloads on which agents cannot be installed.

Agent-based Scan (supported using Cloud native services)

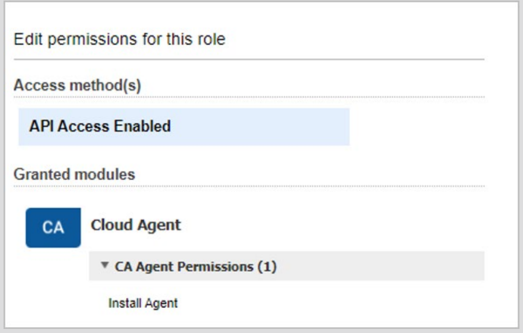
- FlexScan uses the agent embedded in the workload to collect operating system, installed software, and other workload-specific metadata information for vulnerability analysis.
- Automatically installs the agent if it does not detect the Qualys Cloud Agent.
- Since agents can collect much more meta-data it offers the most comprehensive vulnerability coverage.

Zero-touch deployment of Qualys Agent

Qualys Cloud agent deployment on AWS is carried out using the Systems Manager (SSM) document and Run Command. You can directly use public SSM documents provided by Qualys, or you can provision the SSM document using Qualys Flow. For the Run command, you can use Qualys Flow or AWS approach of the SSM State Manager.

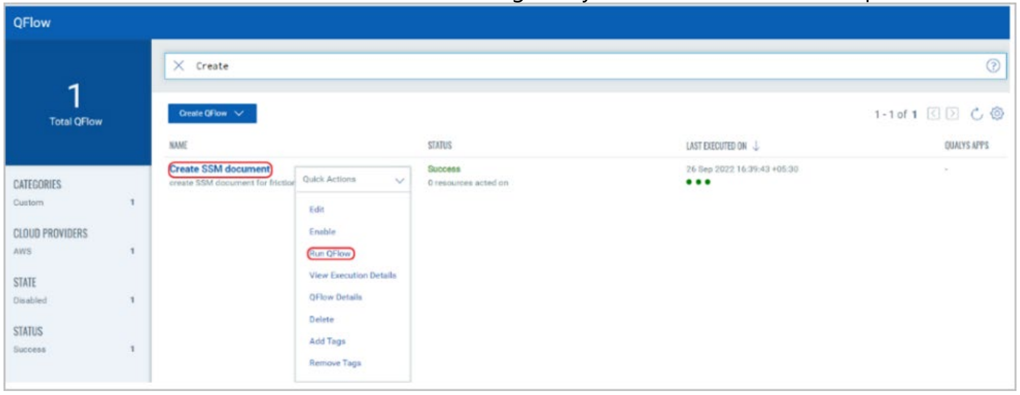
Step 1 – Create Profile

Before you begin with SSM Document Processing and Run command, ensure that the following configurations are in place:

Action	Description
Qualys Cloud Platform subscription with Cloud Agent Module	• ActivationId • CustomerId • WebServerUri • UserName (Qualys API user username) • Password
On the AWS account the following need to be configured	• SSM Agent on the EC2 instance should be installed and running. • EC2 IAM (Identity & Access Management) instance should have proper SSM role attached. • Endpoints need to be created from SSM to the subnet of the EC2 instances.
On the Qualys Admin portal	Create an API user in the Qualys portal with the permission below.  Edit permissions for this role Access method(s) API Access Enabled Granted modules CA Cloud Agent ▾ CA Agent Permissions (1) Install Agent

Step 2 - SSM Document Provisioning

Customer Owned - Use the SSM Document using Qualys Flow out of the box template.

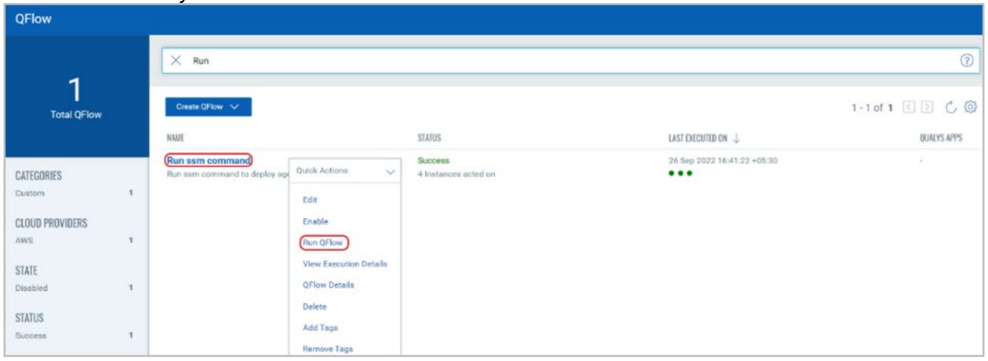


Create

NAME	STATUS	LAST EXECUTED ON	QUALYS APPS
Create SSM document create SSM document for frictior	Success 0 resources acted on	26 Sep 2022 16:39:43 +05:30	-

Step 3-SSM Run Command

- **Run using Qualys Flow** - Qualys Flow provides an out of the box template to run the SSM Document on the EC2 instance. While running the Qualys Flow, go to edit and in the Variable section pass the complete parameters. Then Run the “Run SSM Command” Qualys Flow.

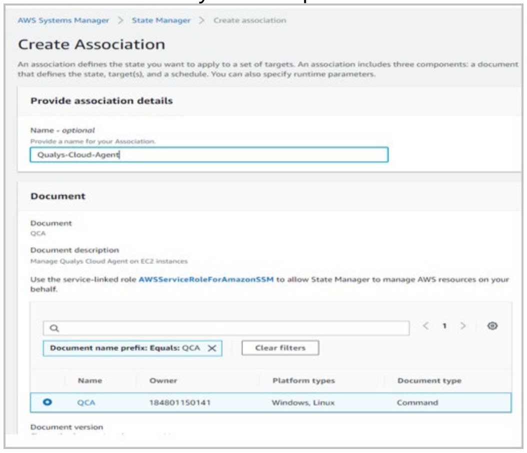


Run

NAME	STATUS	LAST EXECUTED ON	QUALYS APPS
Run ssm command Run ssm command to deploy age	Success 4 Instances acted on	26 Sep 2022 16:41:22 +05:30	-

- **Run using SSM State Manager** - SSM State Manager gives the option to run the SSM document on the EC2 instances based on tags or resource group or on all the EC2 instances based on schedule.

- *AWS System Manager > State Manager* and create association on the SSM Document of Qualys or self-provisioned.



Create Association

An association defines the state you want to apply to a set of targets. An association includes three components: a document that defines the state, target(s), and a schedule. You can also specify runtime parameters.

Provide association details

Name - *optional*
Provide a name for your Association.
Qualys-Cloud-Agent

Document

Document
QCA

Document description
Manage Qualys Cloud Agent on EC2 instances

Use the service-linked role AWSServiceRoleForAmazonSSM to allow State Manager to manage AWS resources on your behalf.

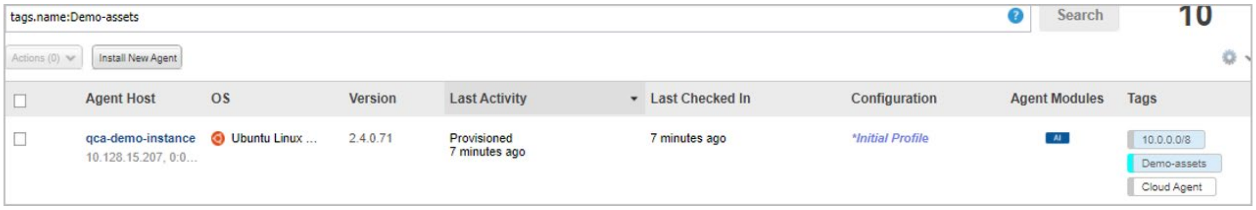
Document name prefix: Equals: QCA

	Name	Owner	Platform types	Document type
●	QCA	184801150141	Windows, Linux	Command

Document version

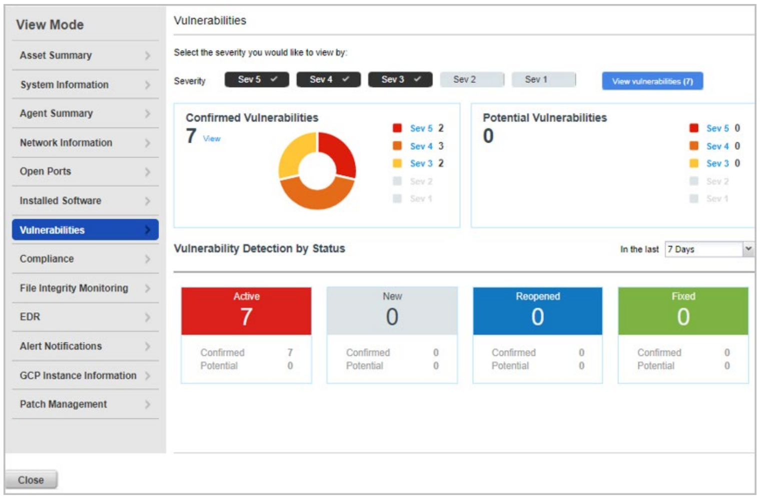
Step 4- Verification

Once all the prerequisites are cleared, using Qualys Flow of SSM State Manager, the SSM document will run on the EC2 instances then the Qualys Cloud Agent is deployed immediately, and it will start showing on Qualys Cloud Platform.



□	Agent Host	OS	Version	Last Activity	Last Checked In	Configuration	Agent Modules	Tags
□	qca-demo-instance 10.128.15.207, 0:0...	Ubuntu Linux ...	2.4.0.71	Provisioned 7 minutes ago	7 minutes ago	*Initial Profile	AI	10.0.0.0/8 Demo-assets Cloud Agent

And when Qualys Cloud Agent performs scan, the Vulnerabilities section starts reflecting vulnerabilities.



Vulnerabilities

Select the severity you would like to view by:

Severity: Sev 5 ✓ Sev 4 ✓ Sev 3 ✓ Sev 2 Sev 1

Confirmed Vulnerabilities 7

🟥 Sev 5	2
🟧 Sev 4	3
🟨 Sev 3	2
Sev 2	
Sev 1	

Potential Vulnerabilities 0

🟥 Sev 5	0
🟧 Sev 4	0
🟨 Sev 3	0
Sev 2	
Sev 1	

Vulnerability Detection by Status — In the last 7 Days

	Active	New	Reopened	Fixed
	7	0	0	0
Confirmed	7	0	0	0
Potential	0	0	0	0

Zero-touch Cloud API Based Scan (Agentless)

Qualys is introducing a different approach to vulnerability management to utilize Cloud native APIs for performing vulnerability assessments. Additionally, cloud inventory is collected in real-time based on events provided by cloud providers.

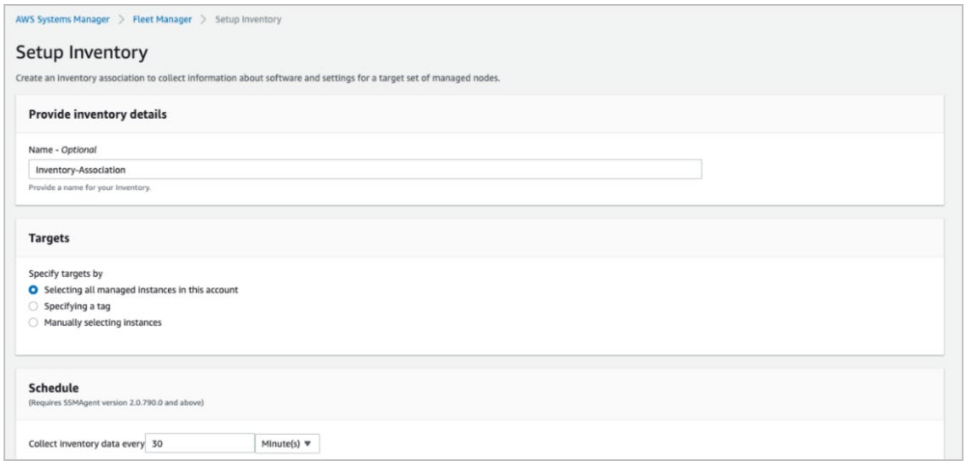
Configuration at AWS Cloud

Customers are required to complete the configurations listed below based on cloud setup.

Step 1- Configure SSM Inventory

SSM inventory can be configured in selected regions or all regions. Follow the below steps to configure it.

Option 1 – Selected region
Login to *AWS Console* > *Navigate to AWS Systems Manager and click Inventory* > *Setup Inventory* > *retain default settings and then click Setup Inventory*.



Setup Inventory

Create an inventory association to collect information about software and settings for a target set of managed nodes.

Provide inventory details

Name - *Optional*: Inventory-Association

Provide a name for your inventory.

Targets

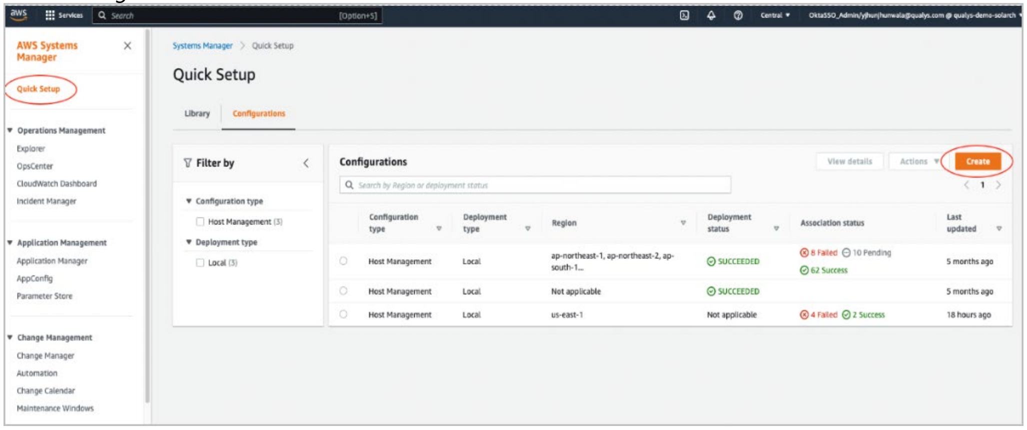
Specify targets by
● Selecting all managed instances in this account
○ Specifying a tag
○ Manually selecting instances

Schedule
(Requires SSMAgent version 2.0.790.0 and above)

Collect inventory data every 30 Minute(s)

Option 2: All regions

1. Login to *AWS Console* > Navigate to *AWS Systems Manager* > *Quick Setup* > click *Create.*
2. *Host Management* > click *Create*.



Quick Setup

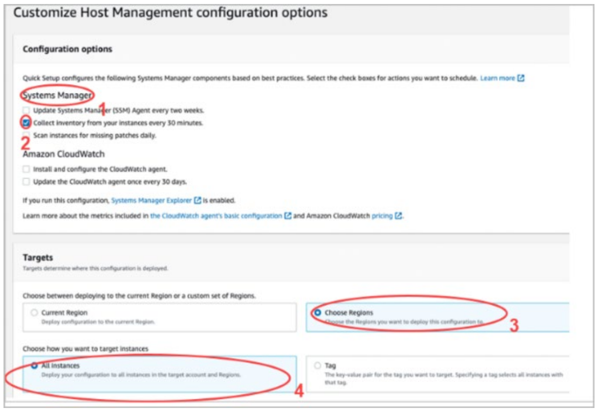
Filter by: Configuration type: □ Host Management (3); Deployment type: □ Local (3)

Configurations

	Configuration type	Deployment type	Region	Deployment status	Association status	Last updated
○	Host Management	Local	ap-northeast-1, ap-northeast-2, ap-south-1...	SUCCEEDED	8 Failed 10 Pending 62 Success	5 months ago
○	Host Management	Local	Not applicable	SUCCEEDED		5 months ago
○	Host Management	Local	us-east-1	Not applicable	4 Failed 2 Success	18 hours ago

After completing the Quick Setup, the next step is customizing Host management configuration options.

1. *Configuration options* > *Systems Manager*.
2. Targets > Choose between deploying to the current Region or a custom set of regions.
3. Targets > Choose how you want to target instances.
4. *Target Regions* > *All Regions*.
5. Click **Create**.



Customize Host Management configuration options

Configuration options

Quick Setup configures the following Systems Manager components based on best practices. Select the check boxes for actions you want to schedule. Learn more

Systems Manager

☐ Update Systems Manager (SSM) Agent every two weeks.

☑ Collect inventory from your instances every 30 minutes.

☐ Scan instances for missing patches daily.

Amazon CloudWatch

☐ Install and configure the CloudWatch agent.

☐ Update the CloudWatch agent once every 30 days.

If you run this configuration, Systems Manager Explorer is enabled.

Learn more about the metrics included in the CloudWatch agent's basic configuration and Amazon CloudWatch pricing.

Targets

Targets determine where this configuration is deployed.

Choose between deploying to the current Region or a custom set of Regions.

○ Current Region — Deploy configuration to the current Region.

● Choose Regions — Choose the Regions you want to deploy this configuration to.

Choose how you want to target instances

● All instances — Deploy your configuration to all instances in the target account and Regions.

○ Tag — The key-value pair for the tag you want to target. Specifying a tag selects all instances with that tag.

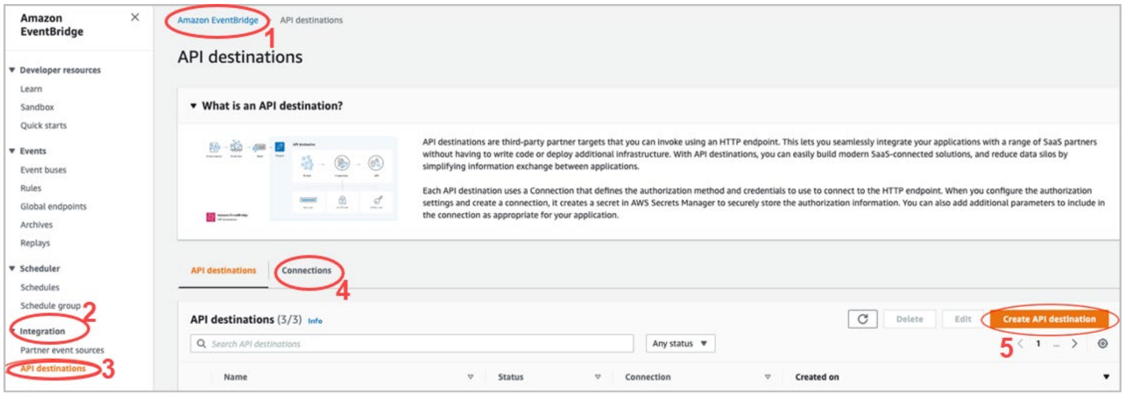
Step 2- Configure EventBridge

Option 1: Manually via AWS Console

Follow the below steps to enable your cloud events to reach the Qualys platform.

API Destination Connection

Login to *AWS Console* > *Navigate to Amazon EventBridge* > *Click Integrations* > *API destinations* > *Connections tabs* > *Create Connection*.



API destinations

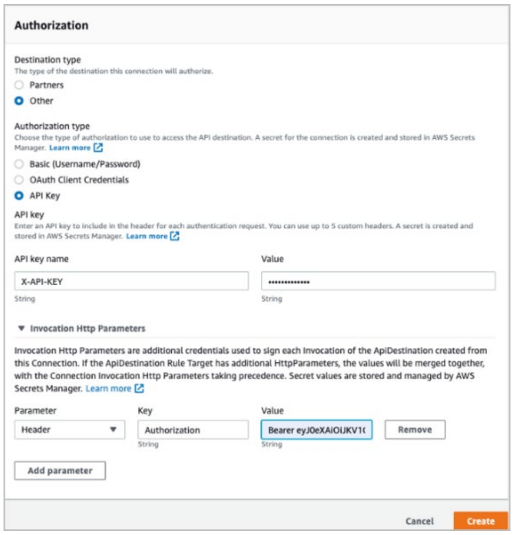
What is an API destination?

API destinations are third-party partner targets that you can invoke using an HTTP endpoint. This lets you seamlessly integrate your applications with a range of SaaS partners without having to write code or deploy additional infrastructure. With API destinations, you can easily build modern SaaS-connected solutions, and reduce data silos by simplifying information exchange between applications.

Each API destination uses a Connection that defines the authorization method and credentials to use to connect to the HTTP endpoint. When you configure the authorization settings and create a connection, it creates a secret in AWS Secrets Manager to securely store the authorization information. You can also add additional parameters to include in the connection as appropriate for your application.

1. Connection Details > Enter the `connection name and description`.
2. Authorization > Destination type > Other.
3. Authorization type > API Key > Enter `API key name and value`.
4. Invocation Http Parameters > Enter `parameter, key, value`.
5. Steps to generate a *Subscription Token* > *Generate Auth token* > *Generate Subscription Token*.

6. Click on **Create**.



Authorization

Destination type
The type of the destination this connection will authorize.
○ Partners
● Other

Authorization type
Choose the type of authorization to use to access the API destination. A secret for the connection is created and stored in AWS Secrets Manager. Learn more
○ Basic (Username/Password)
○ OAuth Client Credentials
● API Key

API key
Enter an API key to include in the header for each authentication request. You can use up to 5 custom headers. A secret is created and stored in AWS Secrets Manager. Learn more

API key name: X-API-KEY (String)
Value: •••••••••••••• (String)

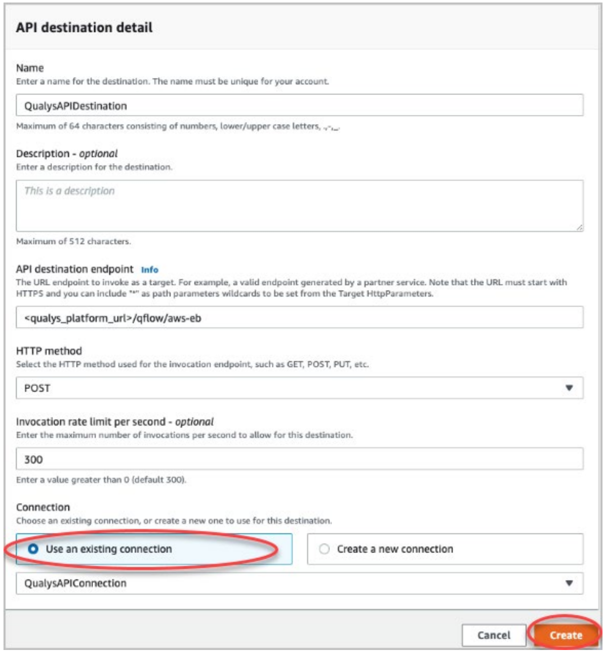
▼ Invocation Http Parameters

Invocation Http Parameters are additional credentials used to sign each Invocation of the ApiDestination created from this Connection. If the ApiDestination Rule Target has additional HttpParameters, the values will be merged together, with the Connection Invocation Http Parameters taking precedence. Secret values are stored and managed by AWS Secrets Manager. Learn more

Parameter	Key	Value
Header	Authorization	Bearer eyJ0eXAiOiJKV1(

API Destination

Click *Integrations >API destinations >API destinations tabs > Create API Destination.*



API destination detail

Name
Enter a name for the destination. The name must be unique for your account.
QualysAPIDestination
Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-,_.

Description - *optional*
Enter a description for the destination.
This is a description
Maximum of 512 characters.

API destination endpoint Info
The URL endpoint to invoke as a target. For example, a valid endpoint generated by a partner service. Note that the URL must start with HTTPS and you can include "*" as path parameters wildcards to be set from the Target HttpParameters.
<qualys_platform_url>/qflow/aws-eb

HTTP method
Select the HTTP method used for the invocation endpoint, such as GET, POST, PUT, etc.
POST

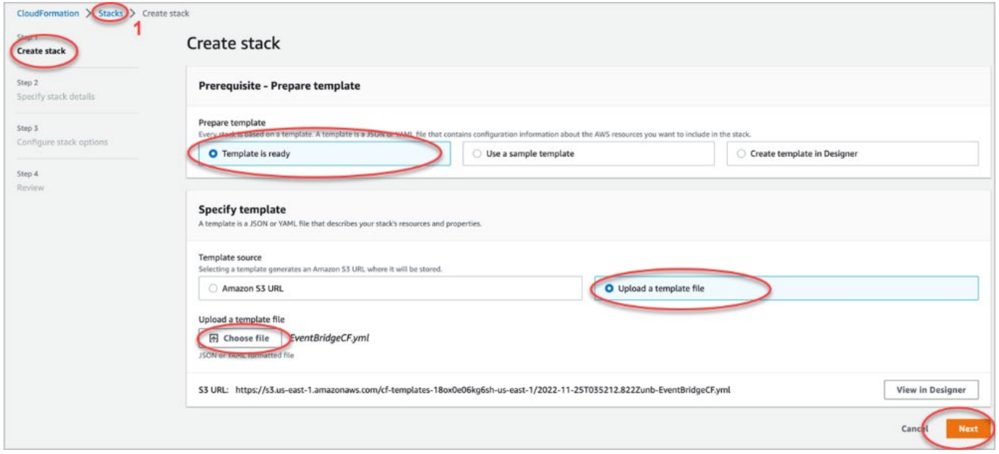
Invocation rate limit per second - *optional*
Enter the maximum number of invocations per second to allow for this destination.
300
Enter a value greater than 0 (default 300).

Connection
Choose an existing connection, or create a new one to use for this destination.
● Use an existing connection ○ Create a new connection
QualysAPIConnection

Option 2: Using AWS CloudFormation Template

1. Login to *AWS Console > Navigate to CloudFormation >Select Stack > Create Stack > With added resources (standard).*
2. Specify *template> Upload a template file > Click Next > Specify stack details.*

3. Template as attached > retain the default settings > Click **Next** > **Submit**.



Create stack

Prerequisite - Prepare template

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

○ Amazon S3 URL ● Upload a template file

Upload a template file

EventBridgeCF.yml

JSON or YAML formatted file

S3 URL: https://s3.us-east-1.amazonaws.com/cf-templates-18ox0e06kg6sh-us-east-1/2022-11-25T035212.822Zunb-EventBridgeCF.yml

Configuration at Qualys Console

We have the following scenarios –

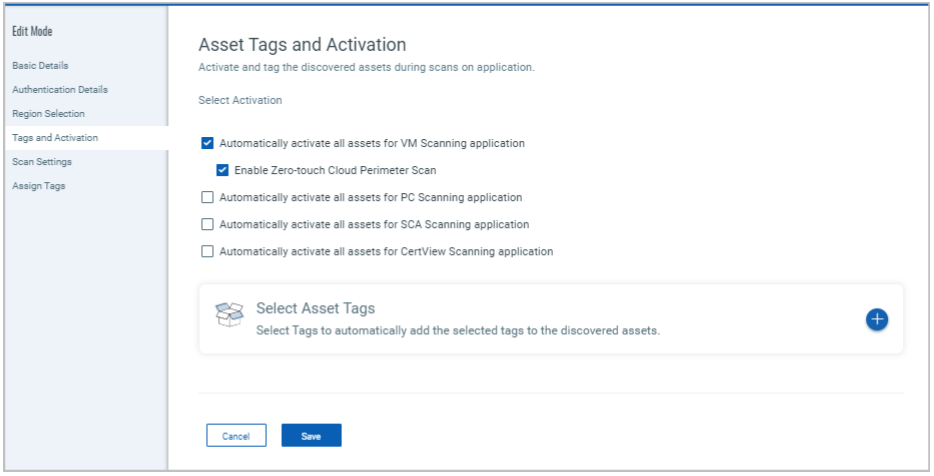
- Connector Application
- TotalCloud Application

Let's deep dive and understand each in detail.

Connector Application

Existing Connector

Login to *Qualys Console* > *Navigate to Connectors Application* > *Amazon Web Services* > *Select Connector* > *Edit* > *Navigate to Tags and Activation.*



Asset Tags and Activation

Activate and tag the discovered assets during scans on application.

Select Activation

☑ Automatically activate all assets for VM Scanning application

☑ Enable Zero-touch Cloud Perimeter Scan

☐ Automatically activate all assets for PC Scanning application

☐ Automatically activate all assets for SCA Scanning application

☐ Automatically activate all assets for CertView Scanning application

Select Asset Tags

Select Tags to automatically add the selected tags to the discovered assets.

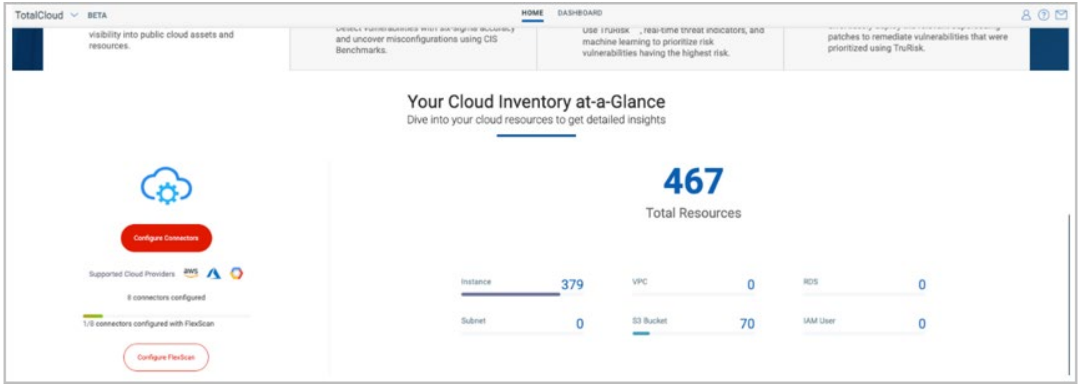
New Connector

Login to *Qualys Console* > *Navigate to Connectors Application* > *Amazon Web Services* > *Create Connector* > *Configure Basic Details i.e., Name, Description, Application* > *Next.*

TotalCloud Application

Existing Connector

Login to *Qualys Console* > *Navigate to TotalCloud* > *Home*> *Click Configure FlexScan.*



visibility into public cloud assets and resources.

and uncover misconfigurations using CIS Benchmarks.

Use TruRisk , real-time threat indicators, and machine learning to prioritize risk vulnerabilities having the highest risk.

patches to remediate vulnerabilities that were prioritized using TruRisk.

Your Cloud Inventory at-a-Glance

Dive into your cloud resources to get detailed insights

Supported Cloud Providers

8 connectors configured

1/8 connectors configured with FlexScan

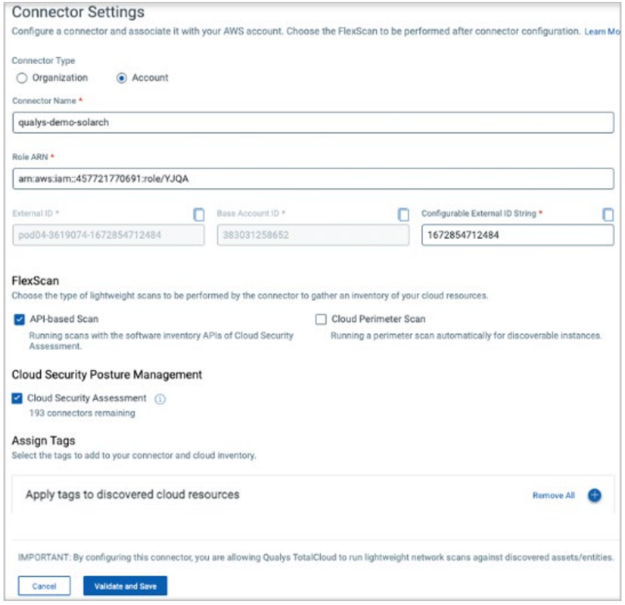
467

Total Resources

Instance	379	VPC	0	RDS	0
Subnet	0	S3 Bucket	70	IAM User	0

New Connector

Login to *Qualys Console* > *Navigate to TotalCloud* > *Configure Connectors* > *Validate and Save.*



Connector Settings

Configure a connector and associate it with your AWS account. Choose the FlexScan to be performed after connector configuration. Learn Mo

Connector Type

○ Organization ● Account

Connector Name *

qualys-demo-solarch

Role ARN *

arn:aws:iam::457721770691:role/YJQA

External ID *

pod04-3619074-1672854712484

Base Account ID *

383031258652

Configurable External ID String *

1672854712484

FlexScan

Choose the type of lightweight scans to be performed by the connector to gather an inventory of your cloud resources.

☑ API-based Scan

Running scans with the software inventory APIs of Cloud Security Assessment.

☐ Cloud Perimeter Scan

Running a perimeter scan automatically for discoverable instances.

Cloud Security Posture Management

☑ Cloud Security Assessment

193 connectors remaining

Assign Tags

Select the tags to add to your connector and cloud inventory.

Apply tags to discovered cloud resources

IMPORTANT: By configuring this connector, you are allowing Qualys TotalCloud to run lightweight network scans against discovered assets/entities.

Zero-Touch Cloud Perimeter Scan

The updated version of the Connector application allows you to secure publicly exposed cloud assets by enabling cloud perimeter scans for your AWS organization connectors. You can create organization (org) connectors for your AWS project connectors in the Connector application.
To learn more about launching Connectors to AWS Organizations and Zero-Touch Cloud Perimeter you can refer to the Release Notes.

To learn more about TotalCloud, visit the product page, watch the video, and sign up for a trial.