AquaSecurity App for Splunk

App Version: 2.0.13

Author: Neel Shah - Greenace Consultants

Description: Installation and Configuration Document for AquaSecurity App for Splunk

Latest Update Date: 22nd Sep, 2021

Version Summary

Version	Change History
1.0.0	Initial Version
2.0.0	Initial Version by Greenace Consultants
2.0.5	Dashboard Revamp, Branding Update, Layout Updates
2.0.7	Minor BugFixes

Supported OS

OS
Windows 10
Windows Server 2012
Windows Server 2016
RHEL 7
RHEL 8
UBUNTU 14
UBUNTU 16
UBUNTU 18
UBUNTU 20

Supported Splunk

Splunk
Splunk 6.X
Splunk 7.X
Splunk 8.X

AquaSecurity App for Splunk

Aqua's comprehensive, purpose-built platform for container security provides full visibility and control over containerized environments, including Kubernetes, OpenShift and Docker.

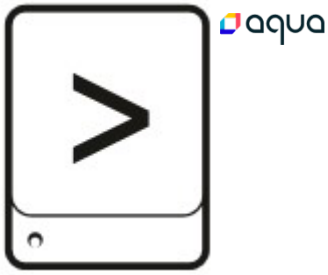
The app shows a security and operational dashboards that is created from audit data collected from Aqua platform.

Install the App

NOTE: There are multiple ways of deploying apps to Splunk environment, in this document we'll be referring installation via CLI (Command Line Interface)

CASE1: SINGLE STAND ALONE MACHINE (CLI)

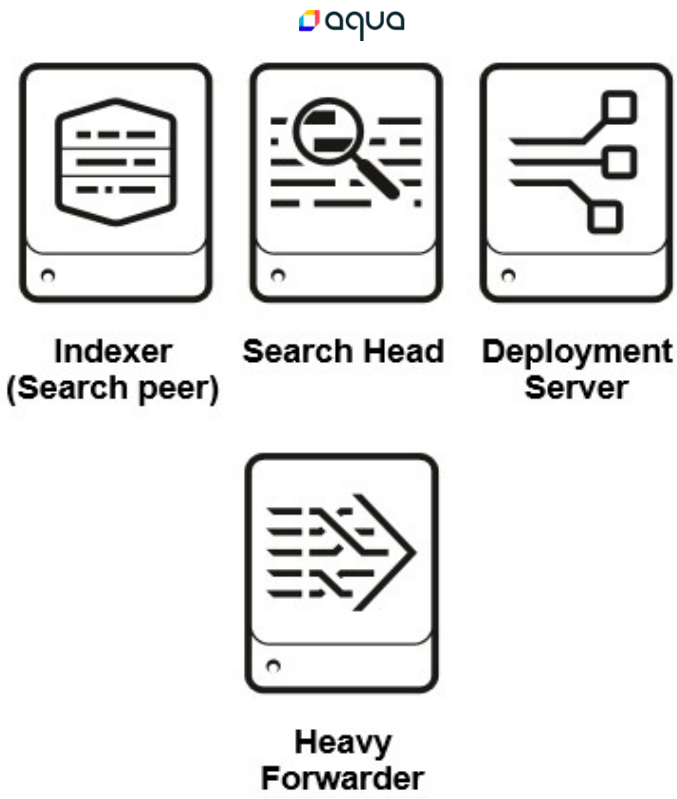
Single standalone Splunk Enterprise Installation on Windows/*NIX



1. **Unzip aqua_security.spl**
2. **Copy** the unzipped directory **aqua_security** to **$SPLUNK_HOME/etc/apps/**
3. **Open CLI** and restart Splunk using **./splunk restart**

CASE2: DISTRIBUTED ARCHITECTURE

Single Indexer Single Search head and Single forwarder (Heavy or Universal) and Deployment server



1. **Unzip aqua_security.spl**
2. **Copy** the unzipped directory **aqua_security** to deployment server in the following location **$SPLUNK_HOME/etc/deployment-apps/**
3. Add following to **serverclass.conf**

   [serverClass:<SEARCHHEAD_SERVERCLASS>:app:< **aqua_security >**]
   stateOnClient=enabled
   restartSplunkd=true

4. **Open CLI** deploy the apps using following command **./splunk reload deploy-server**

CASE3: DISTRIBUTED ARCHITECTURE

Multiple non-clustered Indexers, Multiple non-clustered SearchHeads, Forwarder(Heavy or Universal) and

Deployment server

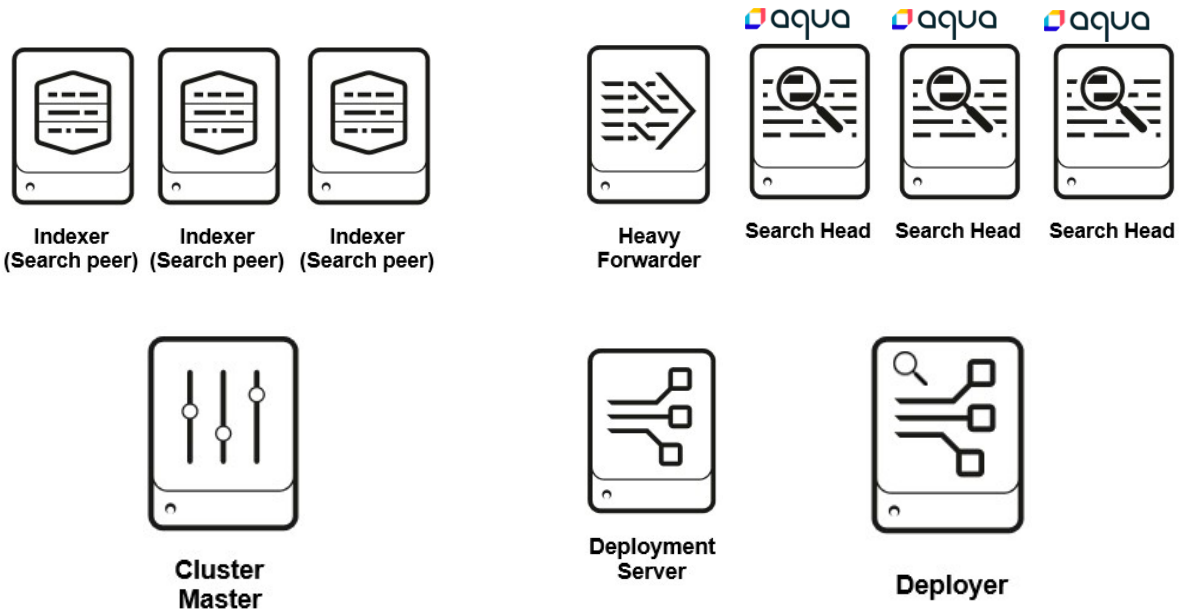
1. **Unzip aqua_security.spl**
2. **Copy** the unzipped directory **aqua_security** to deployment server in the following location **$SPLUNK_HOME/etc/deployment-apps/**
3. Add following to **serverclass.conf**

   [serverClass:<SEARCHHEAD_SERVERCLASS>:app:< **aqua_security** >]
   stateOnClient=enabled
   restartSplunkd=true

4. **Open CLI** deploy the apps using following command **./splunk reload deploy-server**

CASE4: DISTRIBUTED ARCHITECTURE

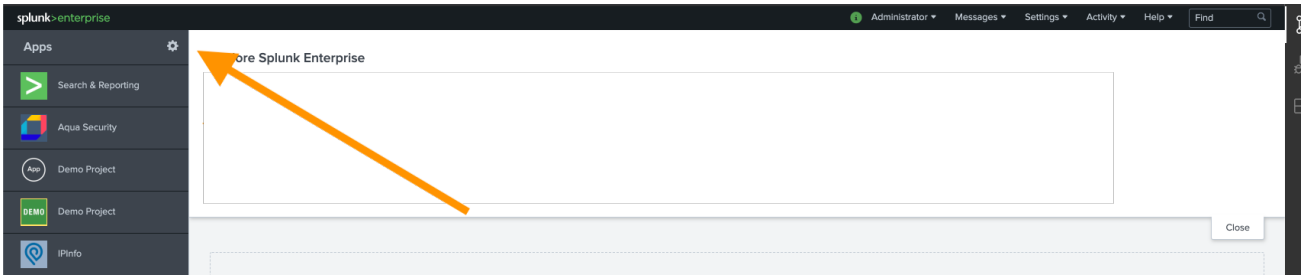
Single Site clustered Indexer, Clustered Search heads and Forwarder (Heavy or Universal).



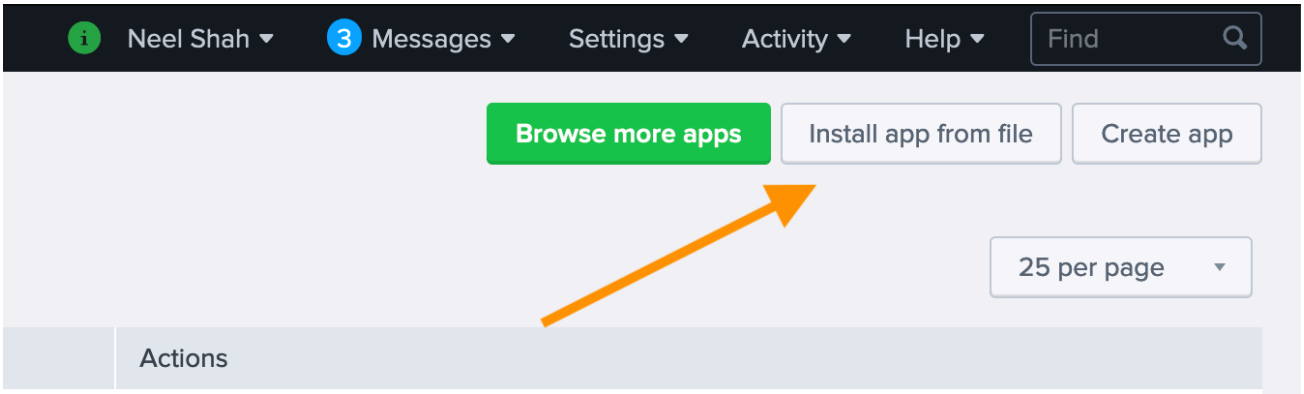
1. **Unzip aqua_security.spl**
2. **Copy aqua_security** to Deployer server in the following location **$SPLUNK_HOME/etc/shcluster/apps/**
3. **Open CLI** on Deployer and deploy the app on Search Head Cluster using following command **./splunk apply shcluster-bundle -target <URI>:<management_port> -auth <username>:<password>**

CASE5: STANDALONE INSTALLATION (WEB)

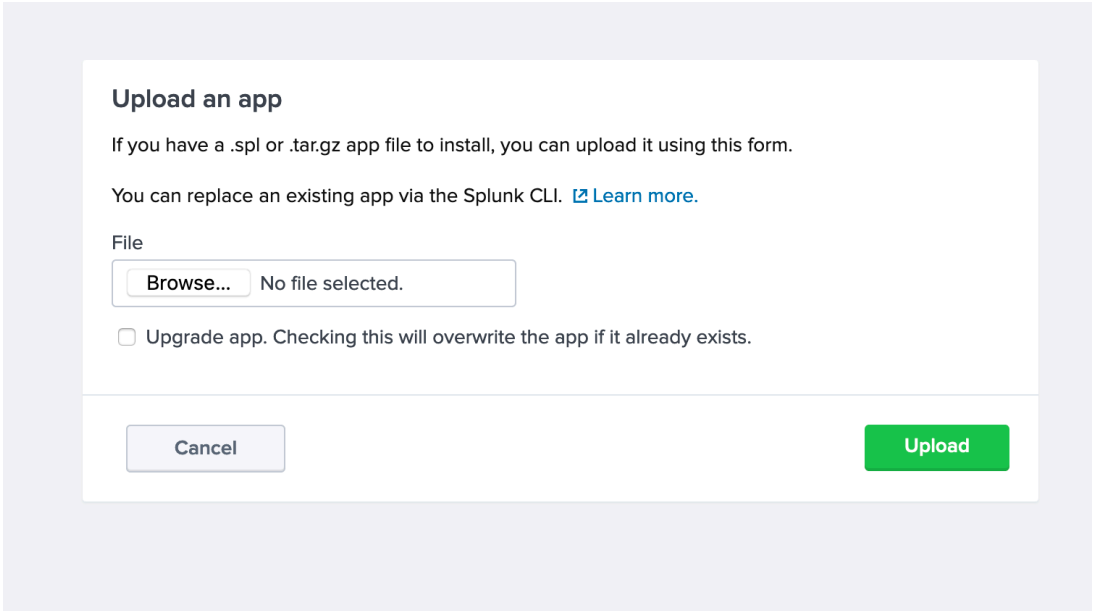
1. On the Splunk Home Page, Click on “Manage Apps”



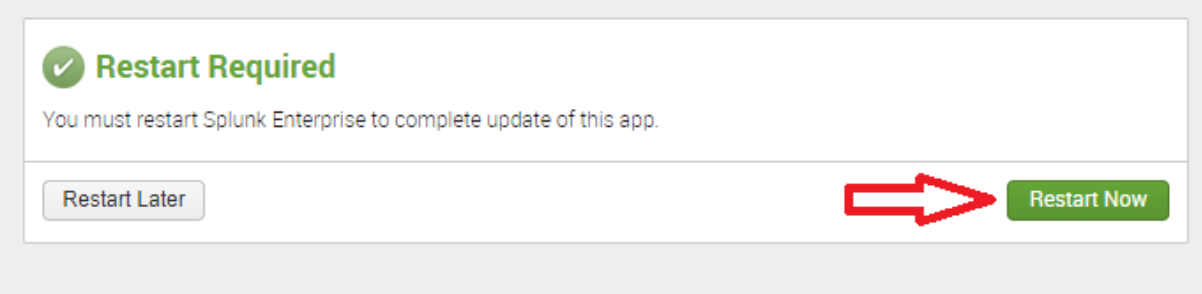
2. On the Manage Apps page, Click on “Install app from file”



3. Select path for Aqua Security Splunk app and Click “Upload”



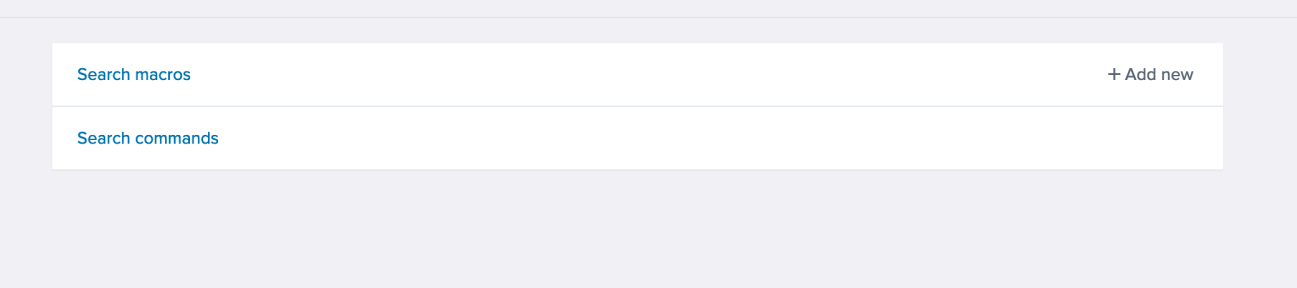
4. Splunk will prompt you to restart the machine, please restart



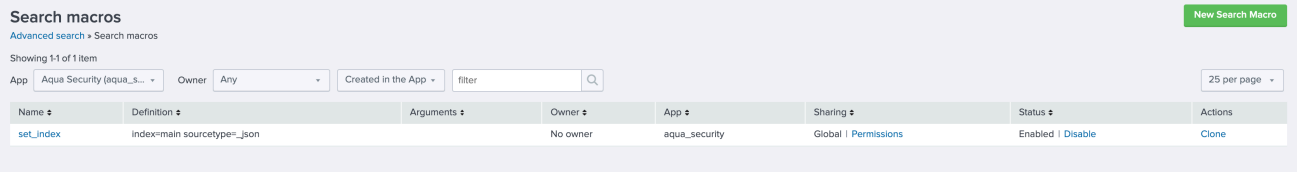
Configuration

1. After Installation and restart, login to the Splunk web and go to ‘Advance Search’

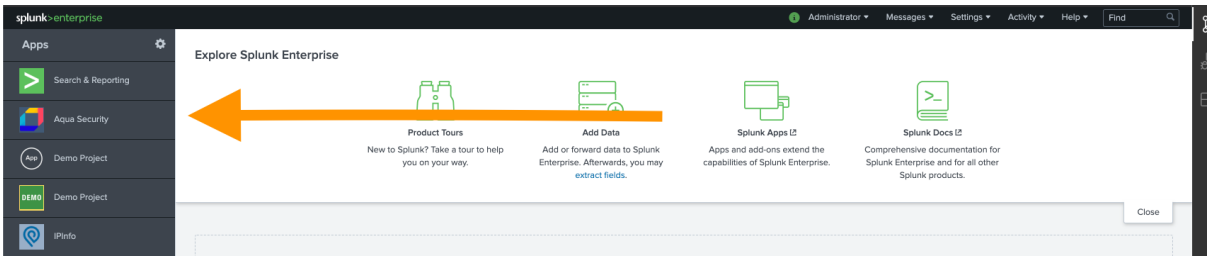
2. Select “Search Macros”



3. Update the Macro and add index and Sourcetype where Aqua Security data is coming

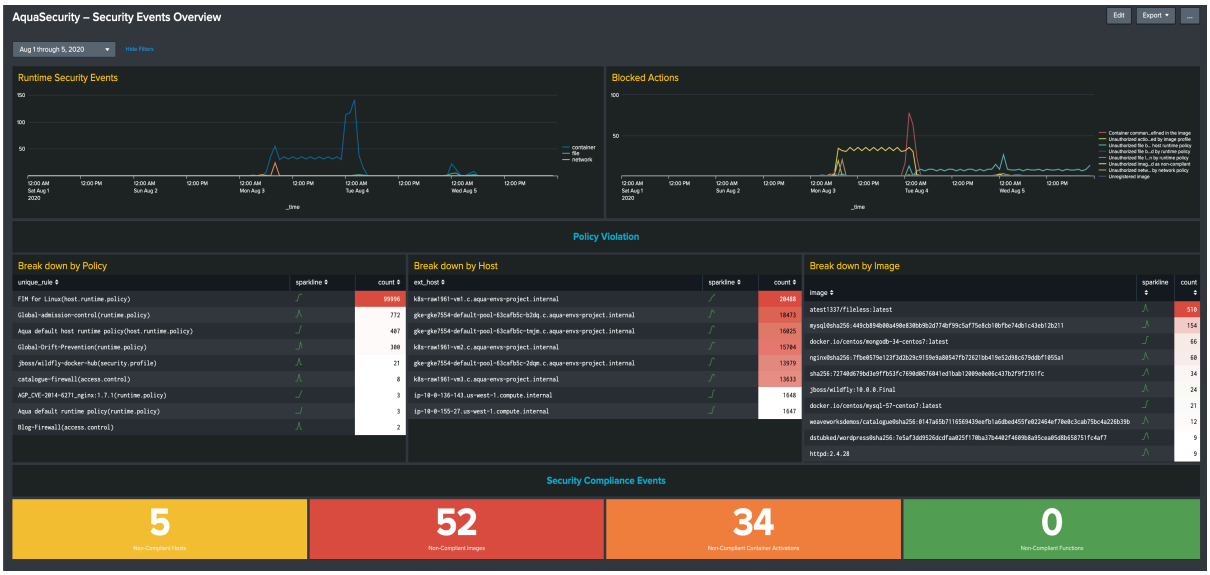


ACCESSING THE APP



Dashboards

AquaSecurity – Security Events Overview



THANK YOU