SecurityBridge

Splunk App

Version 1.1.0

Author: ABAP-Experts.com

Date: 30th April, 2018

Index

Version Summary

Version	Change History
1.0.0	Initial version
1.1.1	Added screenshots and web installation steps

Supported OS

OS
Windows 7
Windows 8
Windows 10
Windows Server 2012
RHEL 6
RHEL 7
UBUNTU 14

SecurityBridge Splunk App

The Splunk SecurityBridge App provides an Integration between SecurityBridge and Splunk.

SAP® is still a blind spot on the security monitoring map for many organizations, as they often assume that their SAP data is covered by the SAP administration team and traditional security methods.

SecurityBridge, a native SAP add-on, gives insight into suspicious activities going wrong within your SAP landscape. This enables you to identify breaches as they occur.

Alerts generated by the SAP SecurityBridge application can be stored on a file share reachable for splunk or FTP'ed to a shared location from where Splunk can read it. Once alert events are loaded in Splunk they can be used to generate reports in the SecurityBridge app. Additionally, data is already compatible with ES app as the data is CIM (4.10.0) compliant.

Install the App

NOTE: There are multiple ways of deploying apps to a Splunk environment. In this document we will be referring to the installation method via the command line interface (CLI)

CASE1: SINGLE STAND ALONE MACHINE (CLI)

Single standalone Splunk Enterprise Installation on Windows / *NIX

1. **Unzip** ***SecurityBridge_App_for_Splunk.spl***

2. **Copy** the unzipped directory **SecurityBridge_App_for_Splunk** 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 *SecurityBridge_App_for_Splunk.spl***

2. **Copy** the unzipped directory **SecurityBridge_App_for_Splunk** to deployment server in the following location ***$SPLUNK_HOME/etc/deployment-apps/***

3. Add following to ***serverclass.conf***

```
[serverClass:<SEARCHHEAD_SERVERCLASS>:app:<
SecurityBridge_App_for_Splunk >] stateOnClient=enabled
restartSplunkd=true

[serverClass:<HEAVYFORWARDER_SERVERCLASS>:app:<SecurityBri
dge_App_for_Splunk>]
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 *SecurityBridge_App_for_Splunk.spl***

2. **Copy** the unzipped directory **SecurityBridge_App_for_Splunk** to deployment server in the following location ***$SPLUNK_HOME/etc/deployment-apps/***

3. Add following to ***serverclass.conf***

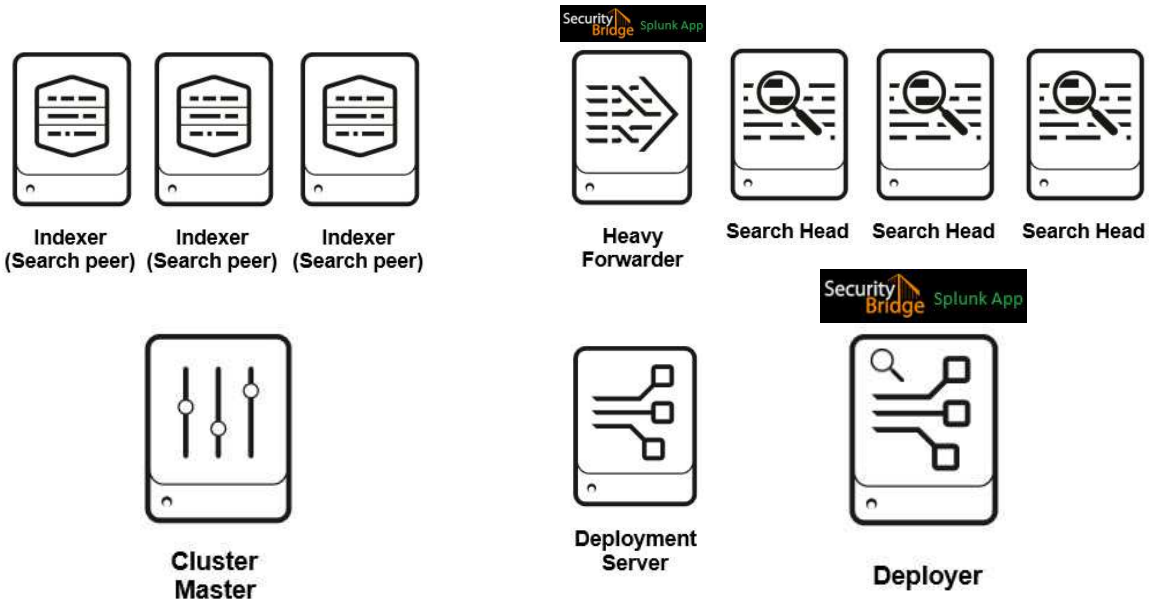
```
[serverClass:<SEARCHHEAD_SERVERCLASS>:app:<
SecurityBridge_App_for_Splunk >] stateOnClient=enabled
restartSplunkd=true

[serverClass:<HEAVYFORWARDER_SERVERCLASS>:app:<SecurityBri
dge_App_for_Splunk>]
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 *SecurityBridge_App_for_Splunk.spl***
2. **Copy SecurityBridge_App_for_Splunk** to Deployer server in the following location ***$SPLUNK_HOME/etc/shcluster/apps/***
3. **Open CLI** on Deployer and deploy the app on Search Head Cluster using following command
   ./splunk apply shcluster-bundle -target <URI>:<management_port> -auth
   <username>:<password>
5. **Copy** the unzipped directory **SecurityBridge_App_for_Splunk** to deployment server in the following location ***$SPLUNK_HOME/etc/deployment-apps/***
6. Add following to ***serverclass.conf***

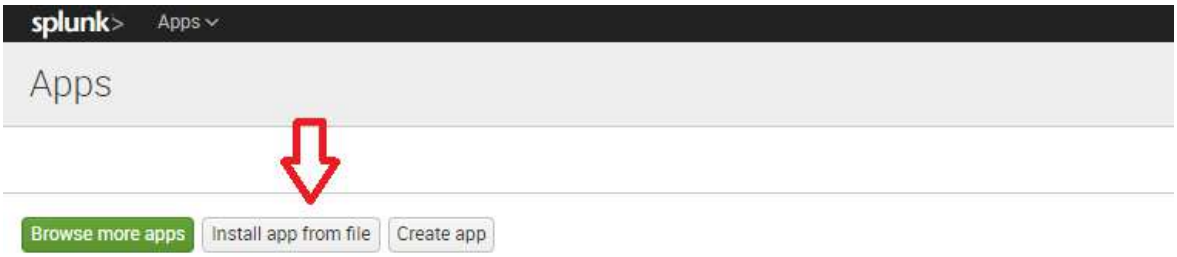
```
[serverClass:<HEAVYFORWARDER_SERVERCLASS>:app:<SecurityBridge_App_for_Splunk>]
stateOnClient=enabled
restartSplunkd=true
```

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

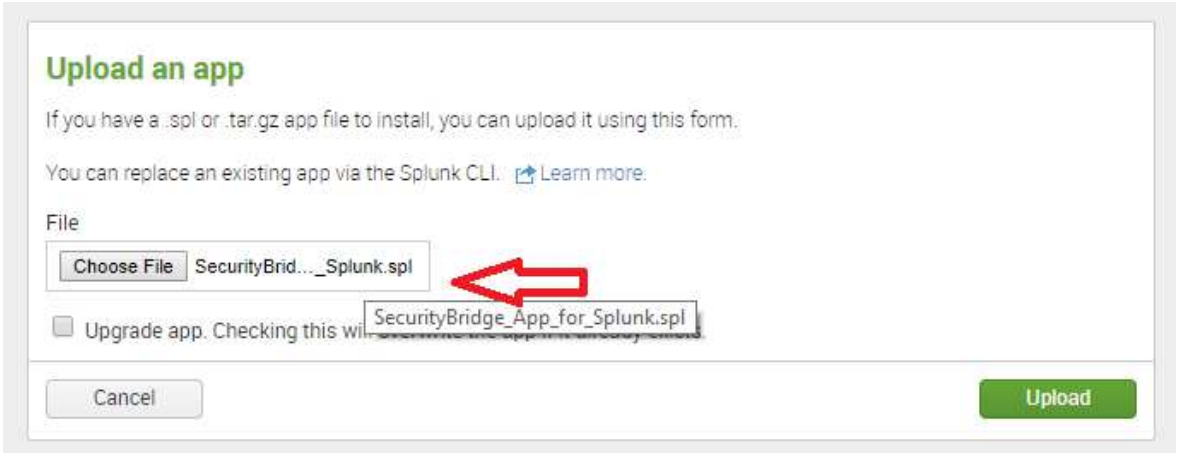
CASE5: STANDALONE INSTALLATION (WEB)

1. On the Splunk Home Page, Click on "*Manage Apps*"

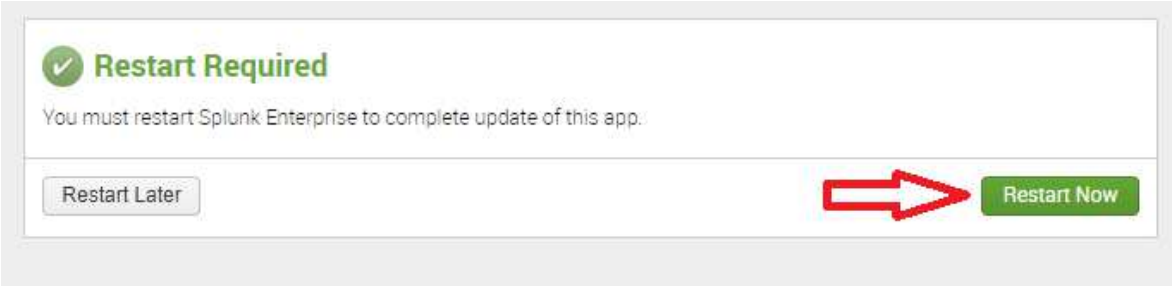
2. On the Manage Apps page, Click on "*Install app from file*"



3. Select path for SecurityBridge Splunk app and Click "Upload"

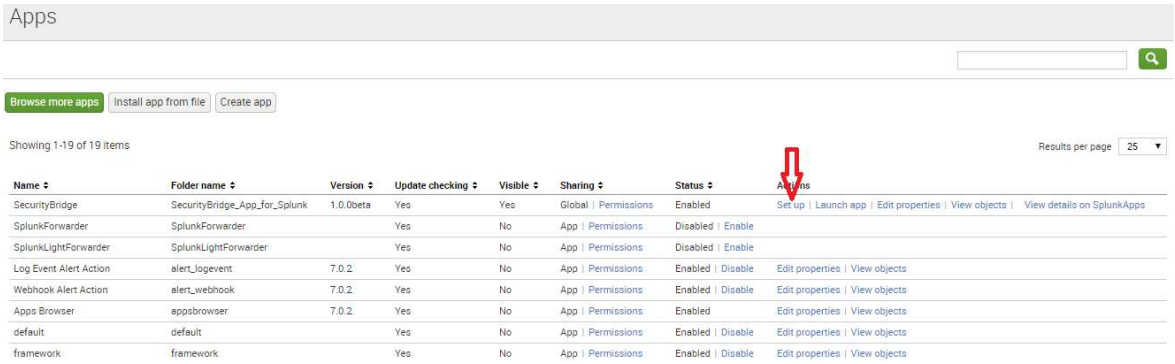


4. Splunk will prompt you to restart the machine, please restart



Configuration

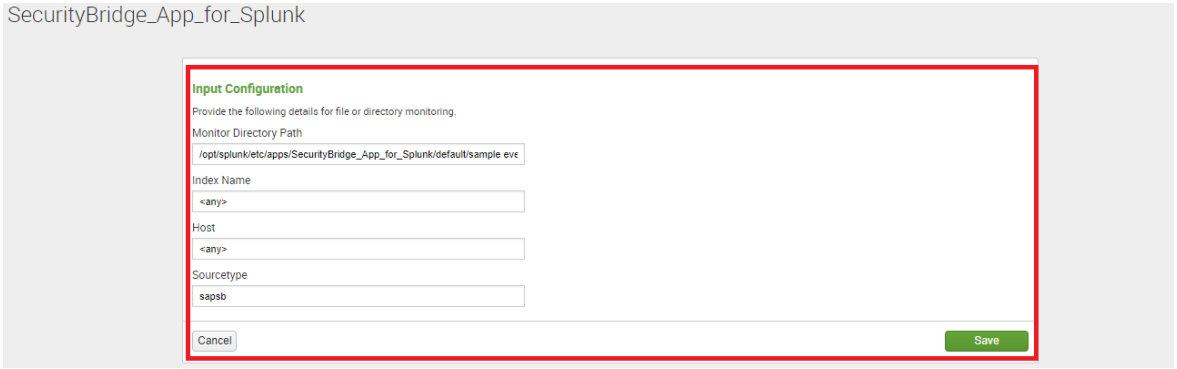
1. After installation and restart, login to the Splunk web and go to '*Manage Apps*'
2. It will list out all the installed application and their configuration option.
3. Look for '*SecurityBridge*' and click on the '*Set-Up*' link to configure the add on.



File Copy Configuration

Follow the below steps to configure the add on.

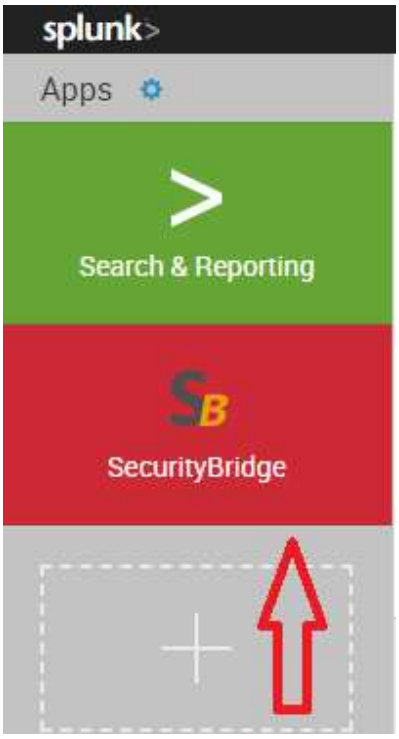
1. The setup link will open a new page, where user needs to enter the details for file copy configuration.



2. As shown in the above screenshot for File Copy configuration provide full directory path of network shared folder. Than select the OS type on which file should be copied. (In case of Windows system, shared directory path should be starting with '\\' and for Linux system it should be starting with '/')

3. Make sure SourceType is **`*sapsb*`**

4. This will complete the setup and you can start using the Security Bridge app.


splunk>
Apps
Search & Reporting
SecurityBridge