

IPInfo App for Splunk

App Version: 3.4.11

Author: Neel Shah - Greenace Consultants

Description: Installation and Configuration Document for IPInfo App for Splunk

Latest Update Date: 13th July, 2020

Version Summary

Version	Change History
1.0.0	Initial Version
1.0.2	Added Screenshots and Web Installation Steps
1.0.3	Replace old dashboard screen with new

Supported OS

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

Supported Splunk

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

IPInfo App for Splunk provides an Integration between IPInfo API and Splunk. This app adds *ipinfo* command to Splunk, which uses IPINFO API engine to lookup information for a given IP

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)

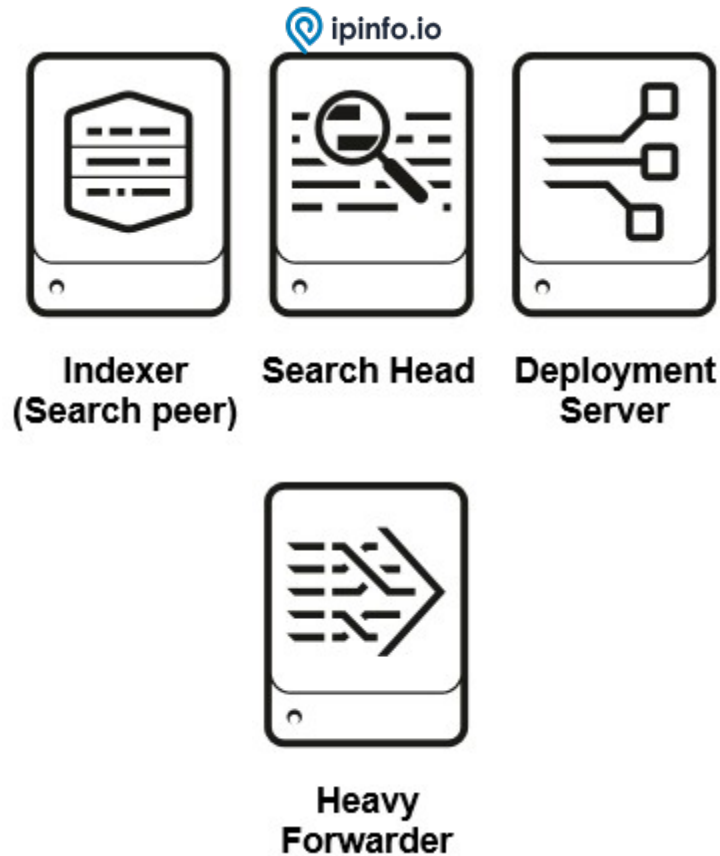
Single standalone Splunk Enterprise Installation on Windows/*NIX



1. **Unzip ipinfo_app.spl**
2. **Copy** the unzipped directory **ipinfo_app** 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



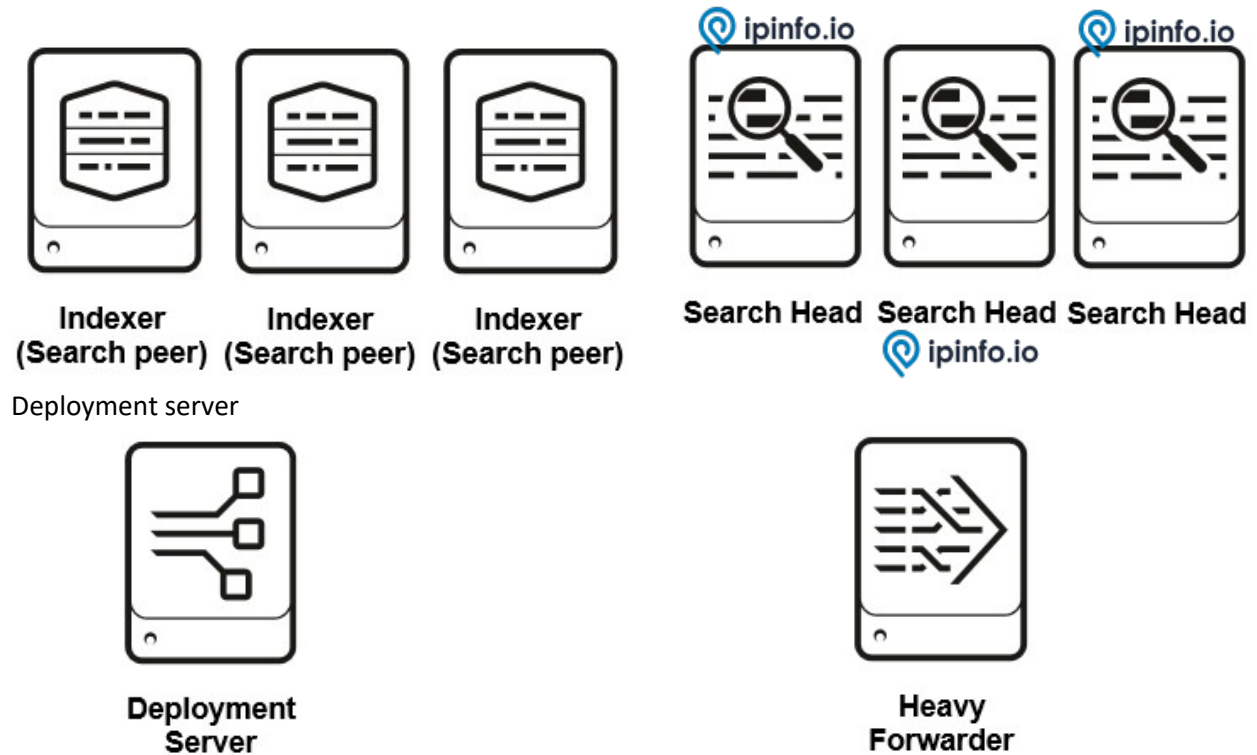
1. **Unzip ipinfo_app.spl**
2. **Copy** the unzipped directory **ipinfo_app** to deployment server in the following location **\$SPLUNK_HOME/etc/deployment-apps/**
3. Add following to **serverclass.conf**

```
[serverClass:<SEARCHHEAD_SERVERCLASS>:app:< ipinfo_app > ]  
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



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

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

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

CASE4: DISTRIBUTED ARCHITECTURE

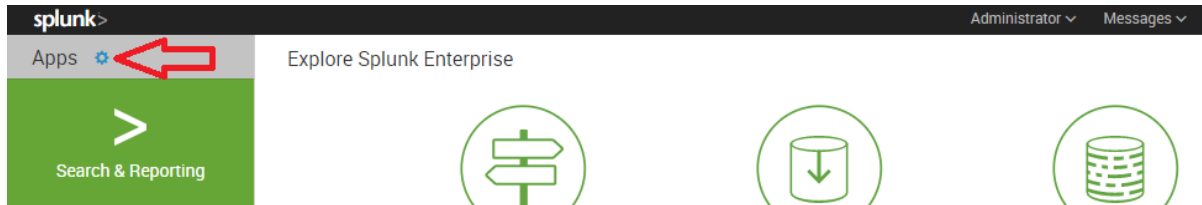
Single Site clustered Indexer, Clustered Search heads and Forwarder (Heavy or Universal).



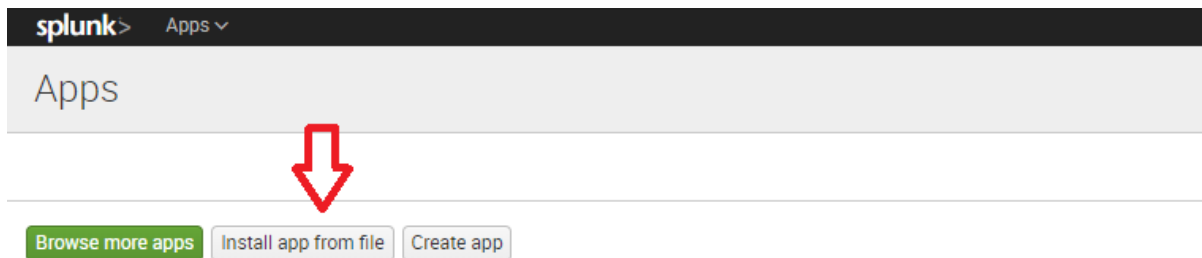
1. **Unzip ipinfo_app.spl**
2. **Copy ipinfo_app** to Deployer server in the following location `$SPLUNK_HOME/etc/shcluster/apps/`
3. **Open CLI** on Deployer and deploy the app on Search Head Cluster using following command
`./splunk apply shcluster-bundle -target <URI>:<management_port> -auth <username>: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

CASE5: STANDALONE INSTALLATION (WEB)

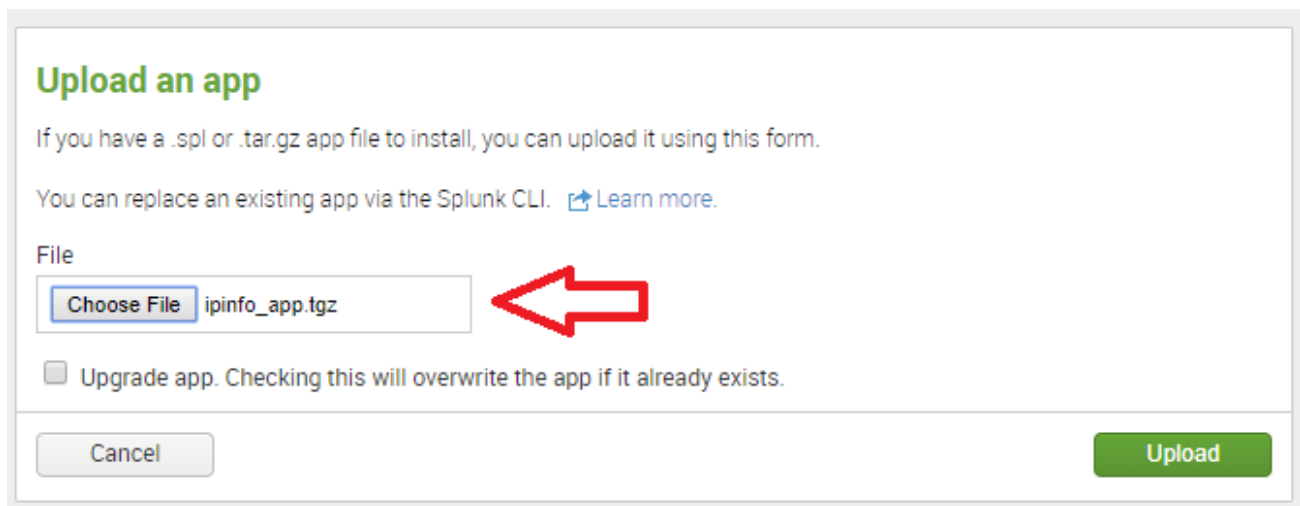
1. On the Splunk Home Page, Click on “Manage Apps”



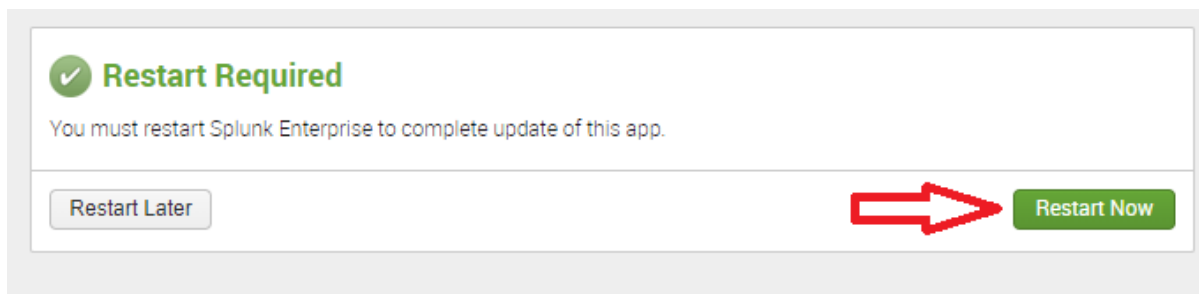
2. On the Manage Apps page, Click on “Install app from file”



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



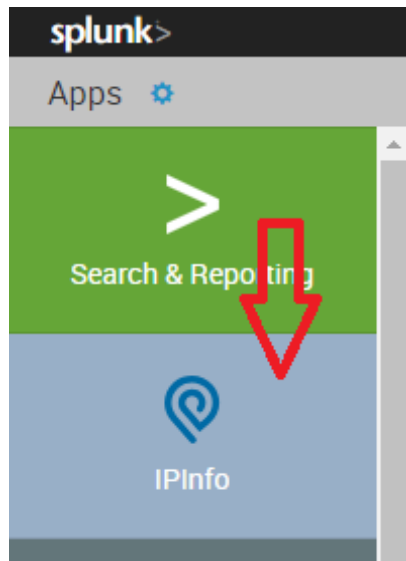
4. Splunk will prompt you to restart the machine, please restart



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 'IPINFO and click on the 'Set-Up' link to configure the add on.
- 4.

and restart Splunk

ACCESSING THE APP



TEST COMMAND

-----IPInfo -----

```
| makeresults 1 | eval ip_add="1.186.41.179" | ipinfo ip_add | table ip, city, region, country, loc, postal, hostname
```

Availability of Fields

- **Basic Subscription** - ip, city, region, country, loc, org, postal, hostname
- **Standard Subscription** - ip, city, region, country, loc, postal, hostname asn_asn, asn_name, asn_domain, asn_route, asn_type
- **Pro Subscription** - ip, city, region, country, loc, postal, hostname asn_asn, asn_name, asn_domain, asn_route, asn_type, company_name, company_domain, company_type, carrier_name, carrier_mcc, carrier_mnc

----- IPInfo Lookup -----

| makeresults | eval

ip="197.94.71.228,197.94.71.227,197.94.71.221,197.94.71.226,197.94.71.225,197.94.71.230" |

makemv delim="," ip | mvexpand ip |lookup ipinfolookup ip

IPInfo

Search

ipinfo.io

Save As ▾Close

New Search

| makeresults | eval ip="197.94.71.228,197.94.71.227,197.94.71.221,197.94.71.226,197.94.71.225,197.94.71.230" | makemv delim="," ip | mvexpand ip |lookup ipinfolookup ip

Last 24 hours ▾

Q

✓ 6 results (7/12/20 9:00:00.000 PM to 7/13/20 9:50:17.000 PM)No Event Sampling ▾

Job ▾|||↗↘⬆⬇⬅

----- IPInfo Batch -----

| ipinfobatch ip="197.94.71.228,197.94.71.227,197.94.71.221 , 197.94.71.226,197.94.71.225 ,197.94.71.22"

New Search

ipinfobatch ip="197.94.71.228,197.94.71.227,197.94.71.221 , 197.94.71.226,197.94.71.225 ,197.94.71.22"

Last 24 hours

✓ 6 results (7/12/20 7:00:00.000 PM to 7/13/20 7:29:56.000 PM) No Event Sampling

Job<

Watch how command works : <https://youtu.be/CaCHgkXvH4M>


IPINFO BASIC

splunk> App: ipinfo Messages Settings Activity Help Find

IPInfo Search ipinfo.io Edit Export ...

139.130.188.239 Hide Filters

139.130.188.239 IP Address		zet1364080.lnk.telstra.net Hostname	
Clarkson City	Western Australia Region	AU Country	6030 Postal



ASN

Full company details are displayed here when you're subscribed to the pro plan.

UPGRADE

COMPANY

Full company details are displayed here when you're subscribed to the pro plan.

UPGRADE

CARRIER

Full company details are displayed here when you're subscribed to the pro plan.


UPGRADE

splunk> App: ipinfo Messages Settings Activity Help Find

IPInfo Search ipinfo.io Edit Export ...

139.130.188.239 Hide Filters

139.130.188.239 IP Address		zet1364080.lnk.telstra.net Hostname	
Clarkson City	Western Australia Region	AU Country	6030 Postal



ASN

Full company details are displayed here when you're subscribed to the pro plan.

UPGRADE

COMPANY

Full company details are displayed here when you're subscribed to the pro plan.

UPGRADE

CARRIER

Full company details are displayed here when you're subscribed to the pro plan.

UPGRADE

About Support File a Bug Documentation Privacy Policy

© 2009-2018 Splunk Inc. All rights reserved.

splunk
App: IPInfo
Messages
Settings
Activity
Help
Find
ipinfo.io

IPInfo
Search
139.130.188.239
Hide Filters

139.130.188.239
IP Address

zet1364080.Ink.telstra.net
Hostname

Clarkson
City

Western Australia
Region

AU
Country

6030
Postal

ASN		COMPANY		CARRIER	
Key	Value	Key	Value	Key	Value
ASN	AS1221	NAME	Telstra Internet	NAME	N/A
NAME	Telstra Pty Ltd	DOMAIN	telstra.com.au	MCC	N/A
DOMAIN	telstra.net	TYPE	isp	MNC	N/A
ROUTE	139.130.0.0/16				
TYPE	isp				

About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2018 Splunk Inc. All rights reserved.

splunk>

App: IPInfo

Messages

Settings

Activity

Help

Find

IPInfo

Search

IPInfo

139.130.188.239

Hide Filters

139.130.188.239

IP Address

zet1364080.lnk.telstra.net

Hostname

Clarkson

City

Western Australia

Region

AU

Country

6030

Postal

+

-

⊕

ASN	COMPANY	CARRIER																												
<table> <tr> <th>Key</th> <th>Value</th> </tr> <tr> <td>ASN</td> <td>AS1221</td> </tr> <tr> <td>NAME</td> <td>Telstra Pty Ltd</td> </tr> <tr> <td>DOMAIN</td> <td>telstra.net</td> </tr> <tr> <td>ROUTE</td> <td>139.130.0.0/16</td> </tr> <tr> <td>TYPE</td> <td>isp</td> </tr> </table>	Key	Value	ASN	AS1221	NAME	Telstra Pty Ltd	DOMAIN	telstra.net	ROUTE	139.130.0.0/16	TYPE	isp	<table> <tr> <th>Key</th> <th>Value</th> </tr> <tr> <td>NAME</td> <td>Telstra Internet</td> </tr> <tr> <td>DOMAIN</td> <td>telstra.com.au</td> </tr> <tr> <td>TYPE</td> <td>isp</td> </tr> </table>	Key	Value	NAME	Telstra Internet	DOMAIN	telstra.com.au	TYPE	isp	<table> <tr> <th>Key</th> <th>Value</th> </tr> <tr> <td>NAME</td> <td>N/A</td> </tr> <tr> <td>MCC</td> <td>N/A</td> </tr> <tr> <td>MNC</td> <td>N/A</td> </tr> </table>	Key	Value	NAME	N/A	MCC	N/A	MNC	N/A
Key	Value																													
ASN	AS1221																													
NAME	Telstra Pty Ltd																													
DOMAIN	telstra.net																													
ROUTE	139.130.0.0/16																													
TYPE	isp																													
Key	Value																													
NAME	Telstra Internet																													
DOMAIN	telstra.com.au																													
TYPE	isp																													
Key	Value																													
NAME	N/A																													
MCC	N/A																													
MNC	N/A																													

About

Support

File a Bug

Documentation

Privacy Policy

© 2015-2018 Splunk Inc. All rights reserved.

splunk>

App: IPInfo

Messages

Settings

Activity

Help

Find

IPInfo

Search

ipinfo.io

Edit

Export

105.4.5.193

Hide Filters

105.4.5.193

IP Address

N/A

Hostname

Germiston

City

Gauteng

Region

ZA

Country

1401

Postal

+

-

ASN	COMPANY	CARRIER
<div>Key</div> <div>Value</div> <div>ASN</div> <div>AS37158</div> <div>NAME</div> <div>Cell C (Pty) Ltd</div> <div>DOMAIN</div> <div>cellc.co.za</div> <div>ROUTE</div> <div>105.4.0/14</div> <div>TYPE</div> <div>isp</div>	<div>Key</div> <div>Value</div> <div>NAME</div> <div>NEOTEL GGSNZ</div> <div>DOMAIN</div> <div>neotel.co.za</div> <div>TYPE</div> <div>isp</div>	<div>Key</div> <div>Value</div> <div>NAME</div> <div>Cell C</div> <div>MCC</div> <div>655</div> <div>MNC</div> <div>7</div>

About

Support

File a Bug

Documentation

Privacy Policy

© 2005-2018 Splunk Inc. All rights reserved.

spunk
App: IPInfo
Messages Settings Activity Help Find
IPInfo Search

Hide Filters

105.4.5.193

IP Address

N/A

Hostname

Germiston

City

Gauteng

Region

ZA

Country

1401

Postal

ASN		COMPANY		CARRIER	
Key	Value	Key	Value	Key	Value
ASN	AS37168	NAME	NEOTEL GGSNZ	NAME	Cell C
NAME	Cell C (Pty) Ltd	DOMAIN	neotel.co.za	MCC	655
DOMAIN	cellc.co.za	TYPE	isp	MNC	7
ROUTE	105.4.0.0/14				
TYPE	isp				

About Support File a Bug Documentation Privacy Policy
© 2005-2018 Splunk Inc. All rights reserved.

THANK YOU