FARSIGHT
SECURITY

FARSIGHT DNSDB APP FOR SPLUNK USER GUIDE

APP VERSION 1.0.0

DATE: FEBRUARY 17, 2016

CONTENTS

Overview..3

About Farsight DNSDB for Splunk..3

Scripts and binaries..4

Release notes..4

About this release..4

Features..5

Third-party software attributions..5

dnsdb lookup Considerations..5

Getting Started..6

Pre-installation checklist..6

Software requirements..6

Splunk Enterprise system requirements..6

Installing Farsight DNSDB App for Splunk..6

Enabling Automatic Lookups in Farsight DNSDB App for Splunk..12

User Guide..16

Usage..16

dnsdb command..16

dnsdblimit command..16

dnsdb lookup..17

Troubleshooting..17

Support and Resources..17

User Guide version: 1.0.0.1001

OVERVIEW

The Farsight DNSDB for Splunk App^{SM} gives organizations of all sizes broad analysis and investigation capabilities. The primary purpose of the Farsight DNSDB for Splunk application is to add contextual information and situational awareness from DNSDB to the organization's internal event data as managed in Splunk.

DNSDB is the most comprehensive database of passive DNS data about how IPs, domains, and Internet infrastructures interconnect and evolve. By augmenting an organization's internal log data with real-time Internet DNS information, security teams will be better able to analyze threats and adversary infrastructure and capabilities. This will enable them to identify, detect, correlate and take action on the intelligence.

All it takes is a simple click in Splunk. With that single click, users can learn the history and infrastructure associated with a suspicious domain name or suspicious IP address, and by doing so, gain critical insights into their event data. Users can also add this capability to their existing workflow to automatically pre-populate contextual information for all IPs and domain names visited by any of their hosts.

With its global array of sensors, Farsight Security receives more than 200,000 observations per second, observations which illuminate most material changes to the global DNS. Farsight DNSDB App for Splunk users get those real-time changes the same minute they are first observed. With more than 13 billion domains and hostnames collected since 2010 – all indexed for easy searches – DNSDB enables threat intelligence teams, security analysts and incident responders to search for specific hosts or subdomains within a domain and gain immediate insight into subordinate names under base domains.

ABOUT FARSIGHT DNSDB FOR SPLUNK

Author:	**Farsight Security, Inc.**
App Version	0.2.2
Vendor Products	Farsight Security DNSDB
Has index-time operations:	False
Create an index:	False
Implements summarization:	False

Farsight DNSDB for Splunk allows a Splunk® Enterprise user to run DNSDB queries from an included dashboard, as well as through search commands.

SCRIPTS AND BINARIES

- dnsdb_query.py
    - Common python module for performing DNSDB queries.
- dnsdb_command.py
    - Splunk custom command for performing DNSDB queries on hostnames/IP addresses.
- dnsdb_ratelimit.py
    - Splunk custom command which retrieves query limit information.
- dnsdb_lookup.py
    - External lookup for querying a set of targets against DNSDB.
    - Note: please see the section titled "dnsdb lookup" before using this.
- dnsdb_validateip.py
    - Internal script used by dashboard to validate IP addresses.
- dnsdb_flushcache.py
    - Internal script used by a daily scheduled search to remove outdated responses from the KV store.

RELEASE NOTES

ABOUT THIS RELEASE

Version 0.2.2 of Farsight DNSDB for Splunk is compatible with:

Splunk Enterprise versions:	6.3, 6.2
CIM	N/A
Platforms	Platform independent
Vendor Products	Farsight Security DNSDB
Lookup file changes	N/A

FEATURES

Version 0.2.2 is the initial release of Farsight DNSDB for Splunk.

It includes the following features:

- Support for various methods of querying DNSDB API:
    - External lookup
    - Custom command
    - Dashboard
- Workflow action to query any field against DNSDB
- Configurable alerts when API key is nearing their daily query quota.

THIRD-PARTY SOFTWARE ATTRIBUTIONS

Version 0.2.2 of Farsight DNSDB for Splunk incorporates the following third-party software or libraries.

- dnsdb-query, https://github.com/dnsdb/dnsdb-query/

DNSDB LOOKUP CONSIDERATIONS

Each DNSDB lookup done takes time to complete. Every event that is passed to it will generate a query to DNSDB. A search for over a few thousand events may take a moment to complete.

Farsight DNSDB API access is capped at a contracted number of queries per day. **Every event passed to the DNSDB lookup will count as a query towards the user's daily quota**. Please be mindful of this when using the lookup functionality so as to not accidentally exhaust your daily query limit. (Should this happen on a regular basis, the query limits can be changed to meet the needs of your threat intelligence team)

GETTING STARTED

PRE-INSTALLATION CHECKLIST

Before installing Farsight DNSDB App for Splunk, please ensure:

1. Your Search Head can access api.dnsdb.info via HTTPS (TCP port 443). If you are a Farsight DNSDB-Export customer, then your Search Head needs to access your local dnstli server.

2. You have administrative privileges within Splunk (our app requires particular permissions).

SOFTWARE REQUIREMENTS

Farsight DNSDB for Splunk can run on Windows, OS X, or Linux.

Farsight DNSDB for Splunk app has no specific additional hardware requirements.

SPLUNK ENTERPRISE SYSTEM REQUIREMENTS

Because this add-on runs on Splunk Enterprise, all of the Splunk Enterprise system requirements apply.

INSTALLING FARSIGHT DNSDB APP FOR SPLUNK

Install the application within Splunk by browsing to

Apps > Manage Apps > Find more apps online,

and searching for Farsight DNSDB.

Or, download the package from Splunkbase at: https://splunkbase.splunk.com/app/3050 and then upload it to your Search Head.

Follow the on-screen installation steps and then restart Splunk.

To install and configure this app on your supported platform, follow these steps:

1. Download app from Splunkbase

   Located at: https://splunkbase.splunk.com/app/3050.

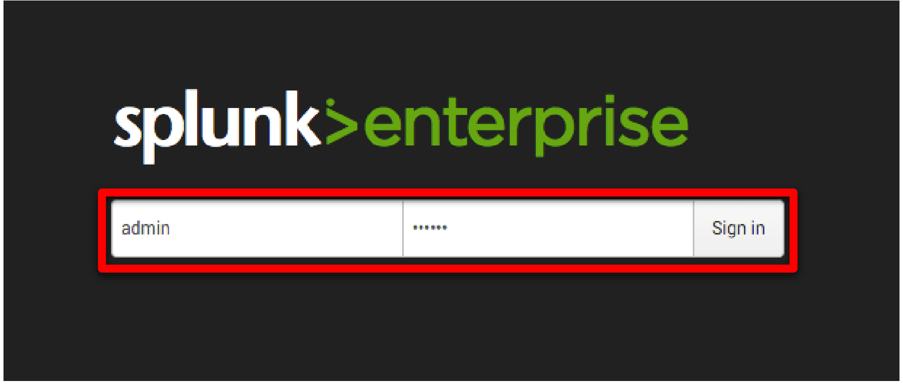
2. Place [app.tar.gz] somewhere on your Search Head

3. Install using splunk command: SPLUNK INSTALL APP /PATH/TO/APP.TAR.GZ

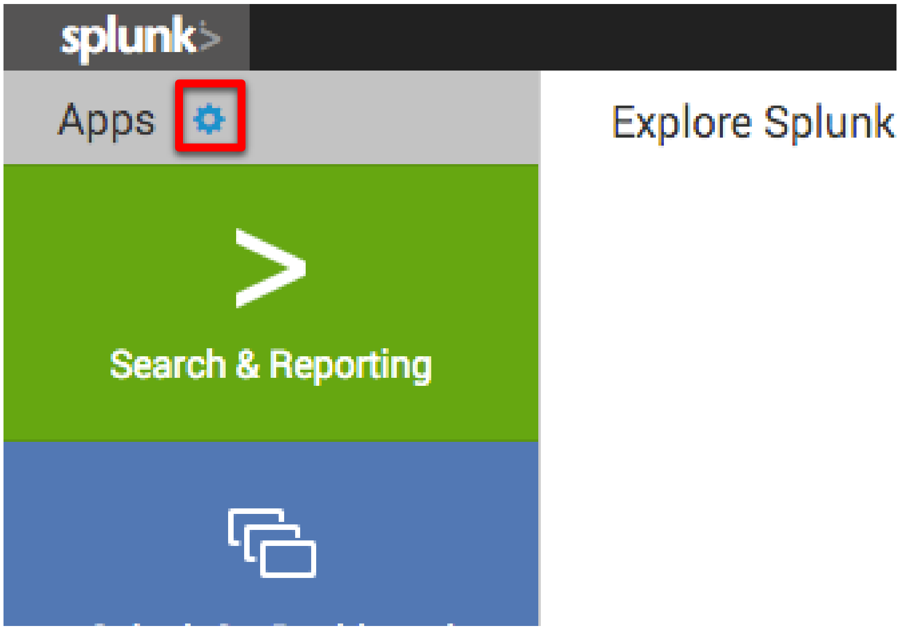
4. Set the DNSDB API key provided by Farsight Security, Inc. This can be done in Splunkweb by clicking "Set up" on the "Manage apps" page, or through the command line by editing dnsdb.conf.

Here are detailed, stepwise instructions to initially set up the Farsight DNSDB for Splunk app.

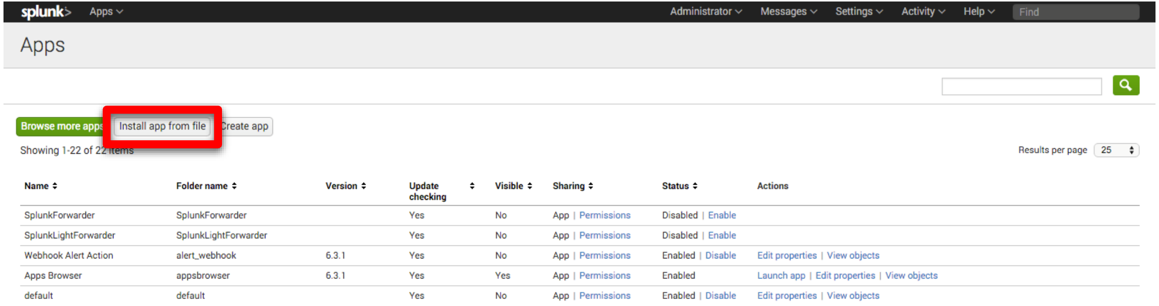
1. Login to your Splunk Enterprise instance as the administrator user.



2. From the entry screen, select the gear icon next to Apps.



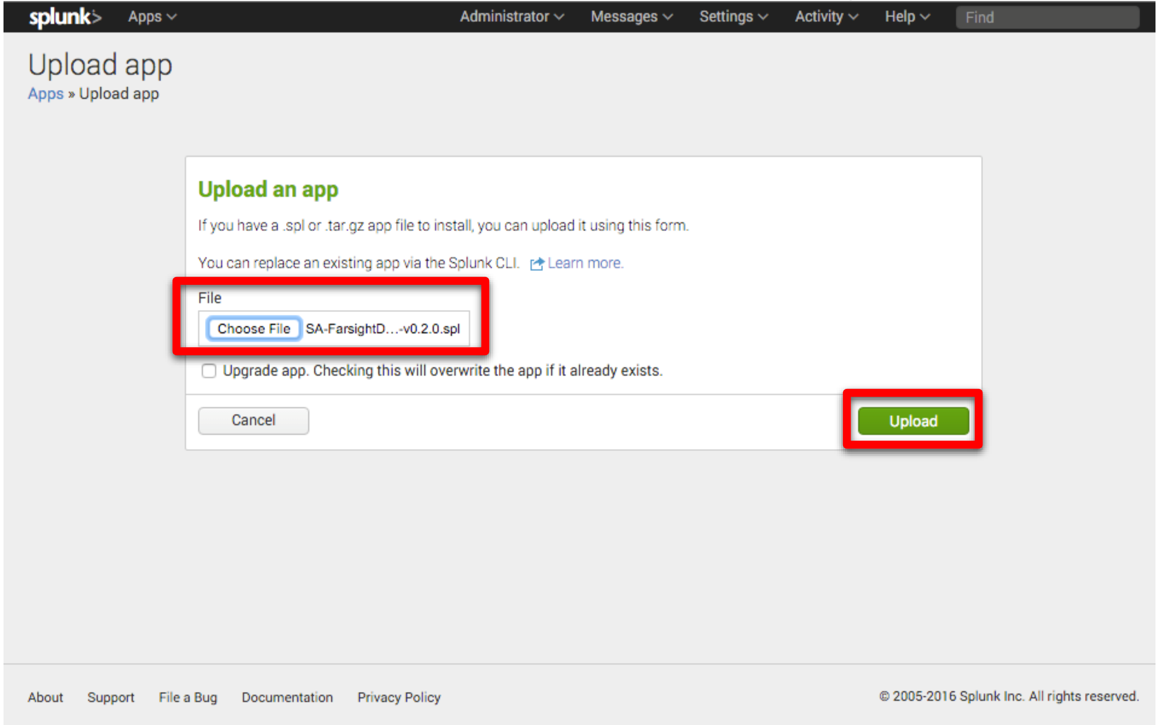
3. Click the [Install app from file] button.



Showing 1-22 of 22 items

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
Webhook Alert Action	alert_webhook	6.3.1	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Apps Browser	appsbrowser	6.3.1	Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
default	default		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects

4. Click the [Choose File] button and select the SPL file provided by Farsight. Click [Upload]



Upload app

Apps » Upload app

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. Learn more.

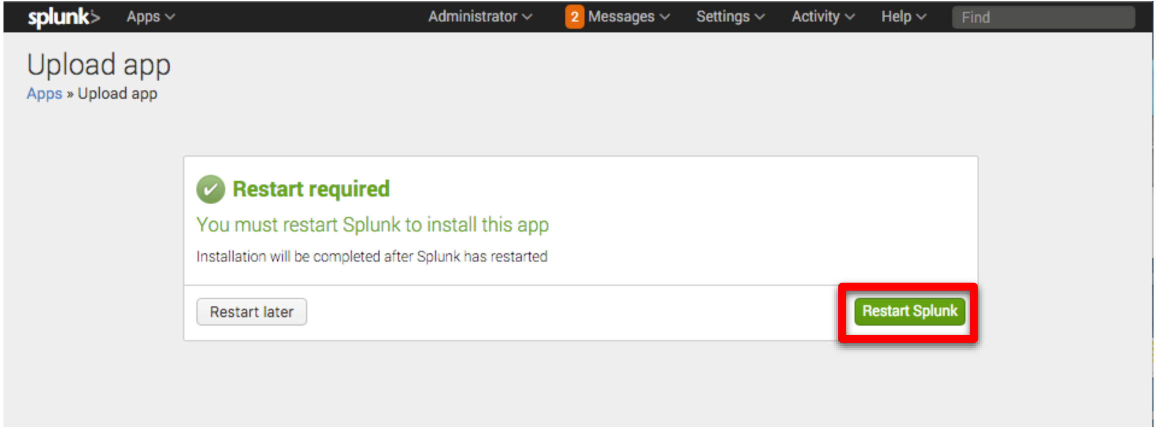
File

Choose File SA-FarsightD...-v0.2.0.spl

□ Upgrade app. Checking this will overwrite the app if it already exists.

© 2005-2016 Splunk Inc. All rights reserved.

5. Installation of the Farsight DNSDB App will require a restart of Splunk. If you wish to restart now, click [Restart Splunk].



Upload app

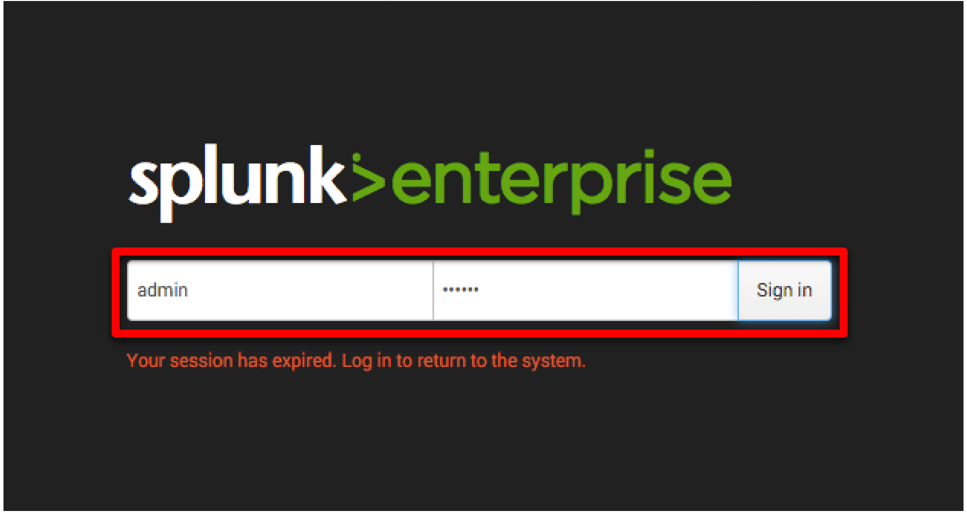
Apps » Upload app

Restart required

You must restart Splunk to install this app

Installation will be completed after Splunk has restarted

6. Once the restart is complete, login as the Administrator user again.

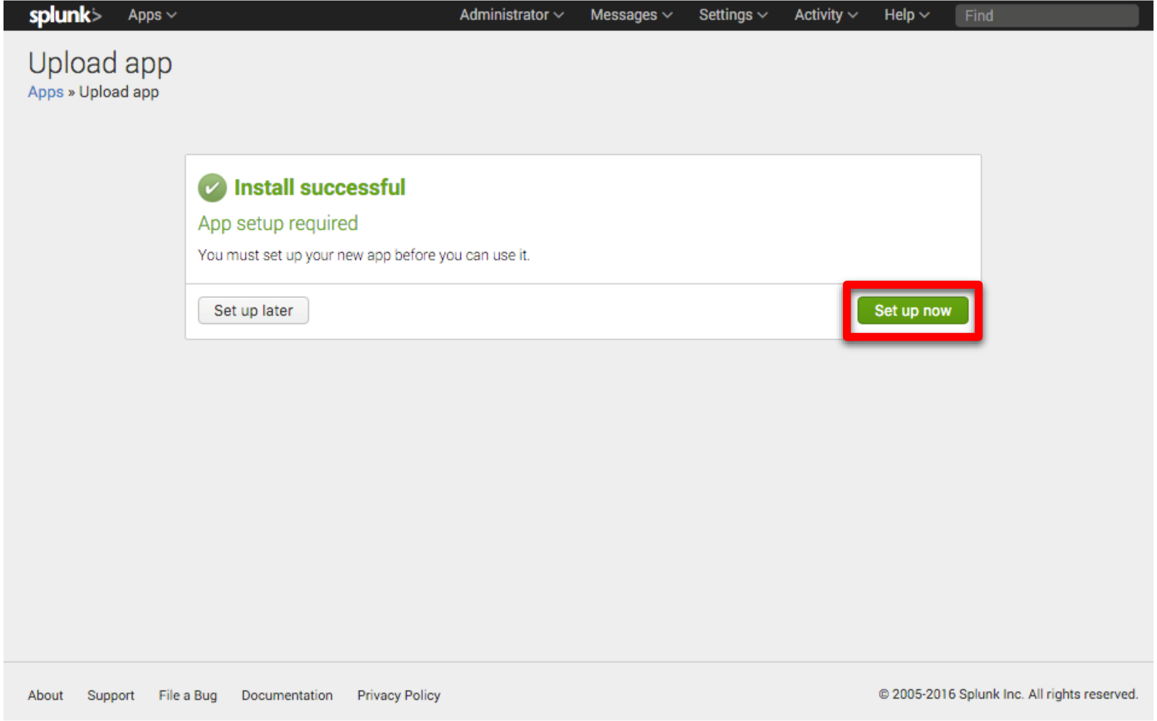


admin

••••••

Your session has expired. Log in to return to the system.

7. Click [Set up now] to configure the Farsight DNSDB App.



Upload app

Apps » Upload app

Install successful

App setup required

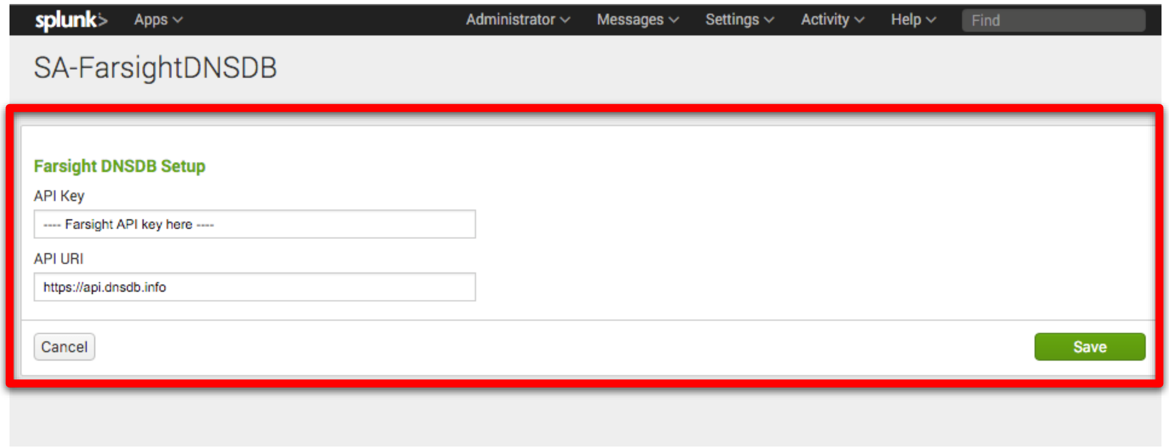
You must set up your new app before you can use it.

© 2005-2016 Splunk Inc. All rights reserved.

8. Enter your Farsight API key. Leave the API URI as: https://api.dnsdb.info

   If you do not have a Farsight API key, please go to: https://www.farsightsecurity.com/trialrequest/?request=splunk

   If you have licensed DNSDB-Export, please change the API URI to the URI used on your export server.



SA-FarsightDNSDB

Farsight DNSDB Setup

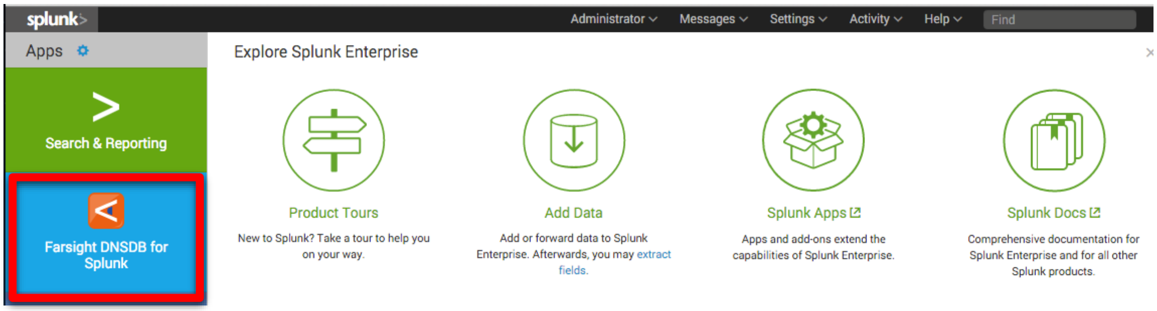
API Key

---- Farsight API key here ----

API URI

https://api.dnsdb.info

9. Click on the Splunk> logo to return to the main screen.
   To access the App, click on [Farsight DNSDB for Splunk].


splunk>
Administrator
Messages
Settings
Activity
Help
Find
Apps
Search & Reporting
Farsight DNSDB for Splunk
Explore Splunk Enterprise
Product Tours
New to Splunk? Take a tour to help you on your way.
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.
Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.
Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

10. You are now ready to use the Farsight DNSDB for Splunk app.

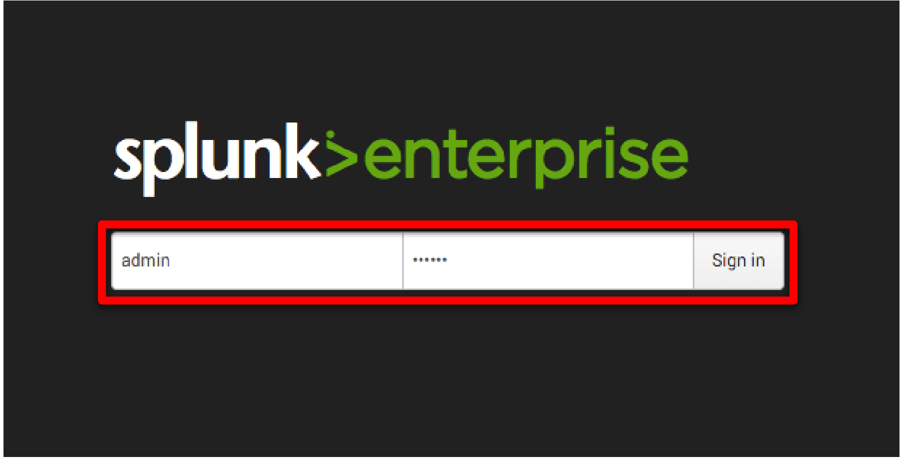
ENABLING AUTOMATIC LOOKUPS IN FARSIGHT DNSDB APP FOR SPLUNK

To provide context for ALL domains and IP addresses within your Splunk instance, you can enable automatic lookups to ensure the information you may need will be immediately ready.

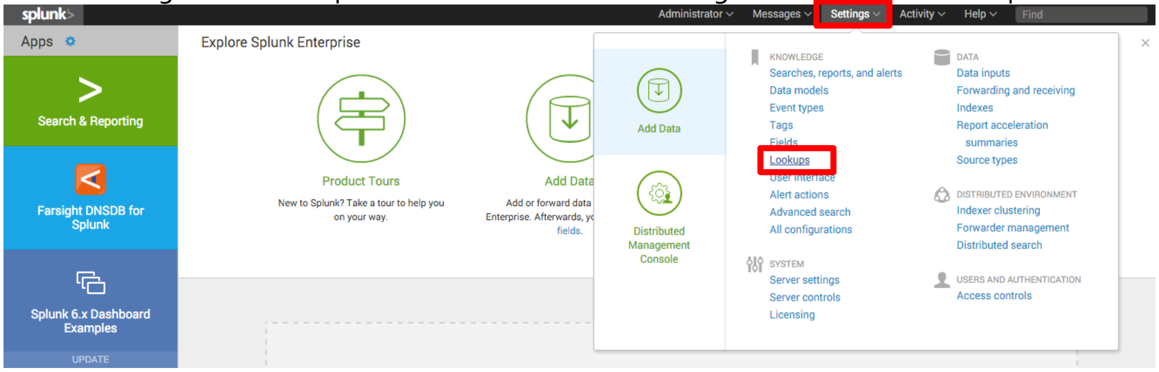
Please note that this will cause a high number of DNSDB queries to occur.

Instructions to enable automatic lookups:

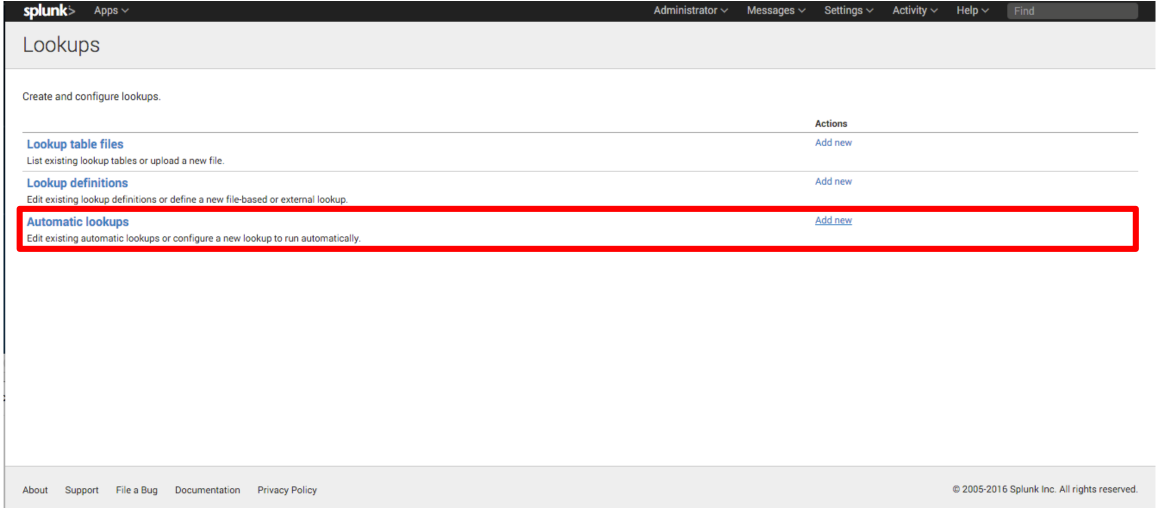
1. Login to your Splunk Enterprise instance as the administrator user.



2. Select Settings from the Top Menu-bar and in the Knowledge section select "Lookups"



3. Find “Automatic lookups”, click “Add new”



Lookups

Create and configure lookups.

	Actions
Lookup table files List existing lookup tables or upload a new file.	Add new
Lookup definitions Edit existing lookup definitions or define a new file-based or external lookup.	Add new
Automatic lookups Edit existing automatic lookups or configure a new lookup to run automatically.	Add new

4. Set the following fields (see attached screenshot for detailed view):

   a. Destination app: For this example we’re going to choose search, you may wish to select something different.

   b. Name: We’re going to call our lookup “ClientIP-DNSDB lookup”

   c. Lookup table: dnsdb

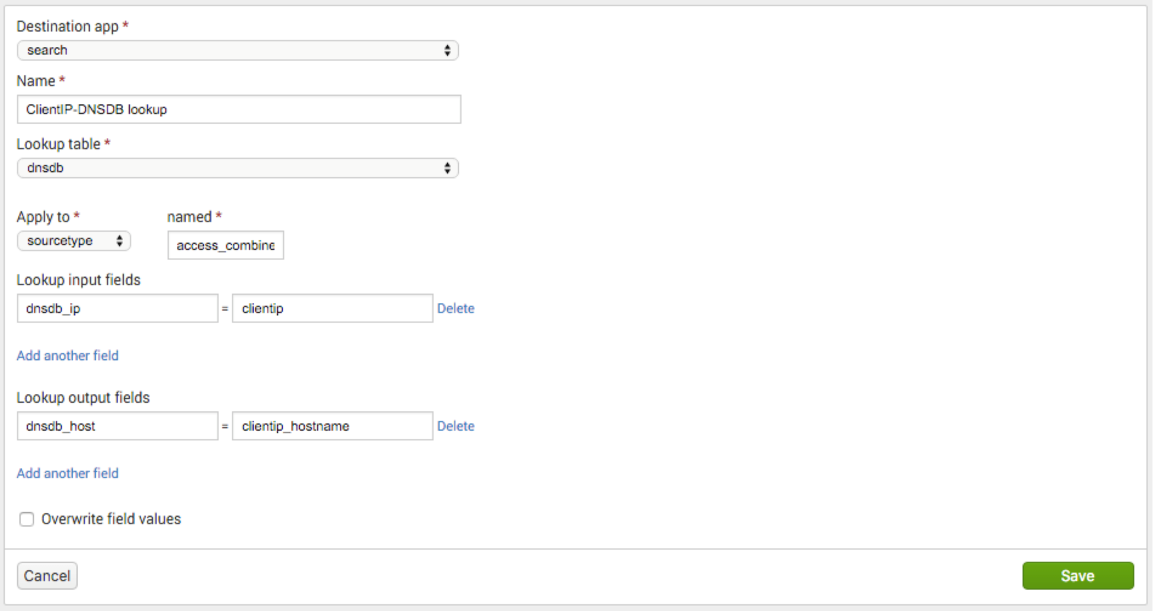
   d. Apply to: sourcetype -> access_combined. This example will make use of combined format weblogs. Select the appropriate for your application.

   e. Lookup input fields: The DNSDB lookup has 2 input fields
      i. dnsdb_host – When the field you wish to act on is a hostname
      ii. dnsdb_ip – When the field you wish to act on is an IP.

      Put the appropriate lookup field in the left-hand input-box. In the right-hand input box enter the name of the field you wish to lookup in your event. In our case it is “clientip”.

   f. Lookup output fields: The output of lookup will be called dnsdb_host, put that in the left-hand box. We want the output to appear as clientip_hostname so that goes in the right-hand field.

   g. Click [Save]



Destination app * search

Name * ClientIP-DNSDB lookup

Lookup table * dnsdb

Apply to * sourcetype named * access_combine

Lookup input fields

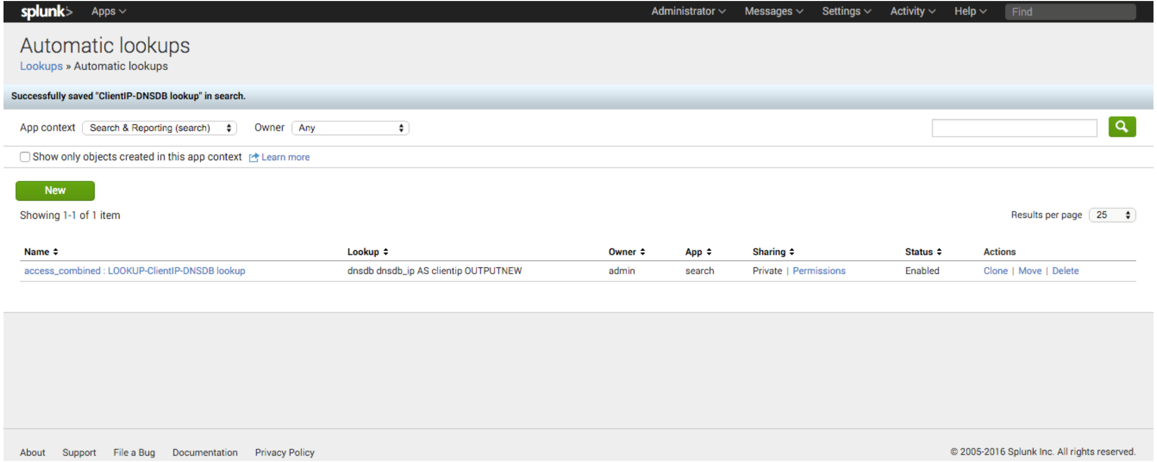
dnsdb_ip = clientip

Lookup output fields

dnsdb_host = clientip_hostname

□ Overwrite field values

5. It should look something like this:



Automatic lookups

Lookups » Automatic lookups

Successfully saved "ClientIP-DNSDB lookup" in search.

App context Search & Reporting (search) Owner Any

□ Show only objects created in this app context

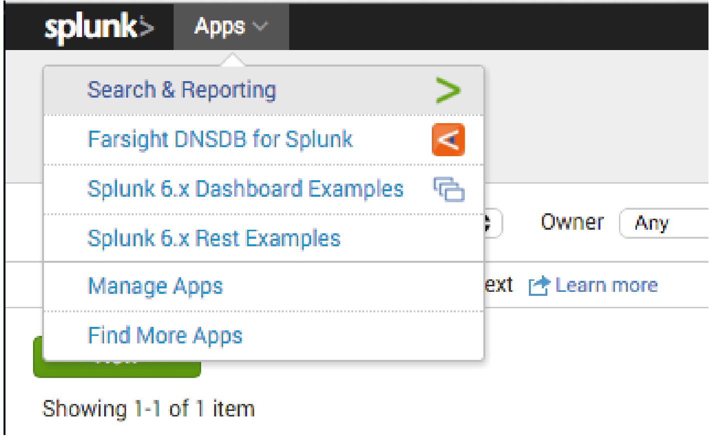
Showing 1-1 of 1 item

Results per page 25

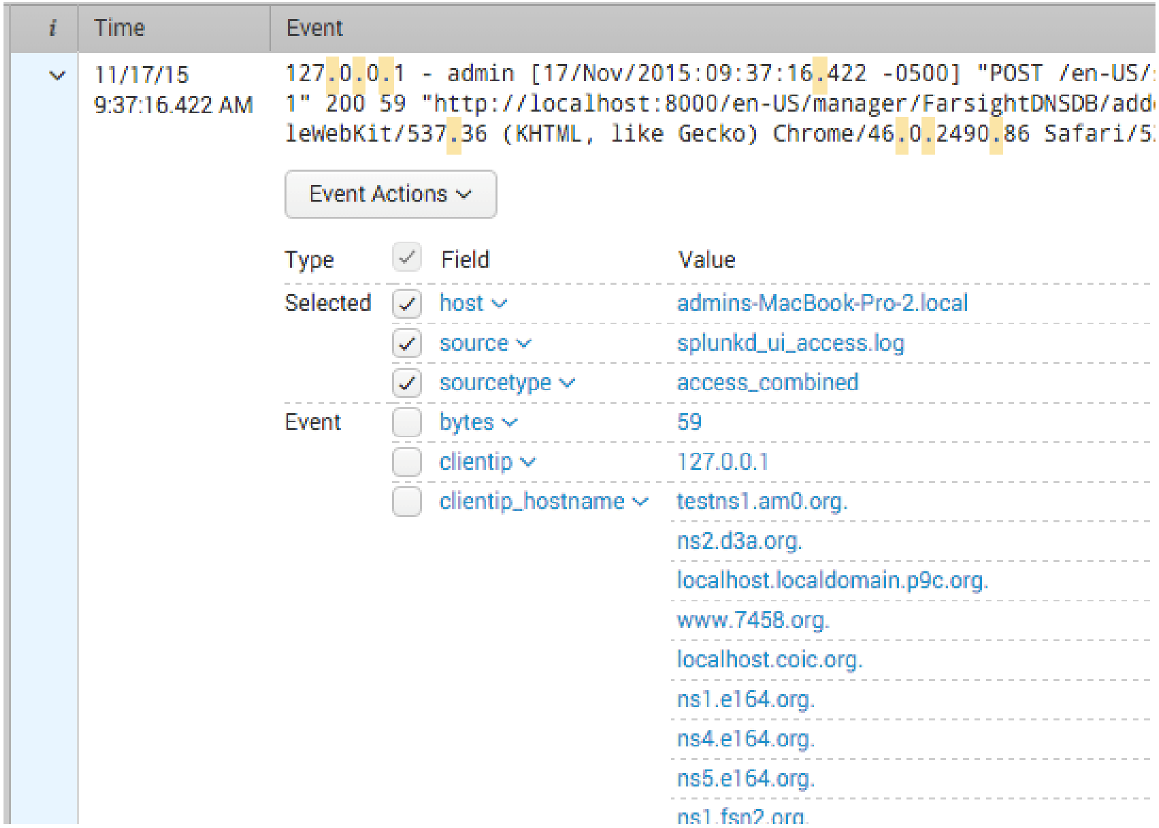
Name	Lookup	Owner	App	Sharing	Status	Actions
access_combined : LOOKUP-ClientIP-DNSDB lookup	dnsdb dnsdb_ip AS clientip OUTPUTNEW	admin	search	Private | Permissions	Enabled	Clone | Move | Delete

© 2005-2016 Splunk Inc. All rights reserved.

6. Return to the main page and open search.



7. Search for “.”



i	Time	Event
⌄	11/17/15 9:37:16.422 AM	

```
127.0.0.1 - admin [17/Nov/2015:09:37:16.422 -0500] "POST /en-US/:
1" 200 59 "http://localhost:8000/en-US/manager/FarsightDNSDB/add
leWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/5
```

Type	✓	Field	Value
Selected	☑	host ⌄	admins-MacBook-Pro-2.local
	☑	source ⌄	splunkd_ui_access.log
	☑	sourcetype ⌄	access_combined
Event	□	bytes ⌄	59
	□	clientip ⌄	127.0.0.1
	□	clientip_hostname ⌄	testns1.am0.org.
			ns2.d3a.org.
			localhost.localdomain.p9c.org.
			www.7458.org.
			localhost.coic.org.
			ns1.e164.org.
			ns4.e164.org.
			ns5.e164.org.
			ns1.fsn2.org.

8. The Farsight DNSDB for Splunk app will now automatically do a lookup for each domain and IP address.

USER GUIDE

USAGE

Once configured, the easiest way to use this app is through the built-in DNSDB dashboard. Choose a time range, type an IP address or hostname into the target field and press enter.

Farsight DNSDB for Splunk also comes with two commands and a lookup so that you can incorporate DNSDB queries into your own searches and dashboards. Below is usage documentation for all three of them.

DNSDB COMMAND

Runs a DNSDB query on the given target. If target is an IP address, query is RDATA. Otherwise, query is RRSET. "before" and "after" fields can be supplied optionally to limit the time range of the query.

Syntax

```
DNSDB TARGET=**IP/HOSTNAME** TYPE=**RDATA/RRSET**
[RRTYPE=**A/MX/CNAME/ETC] [EARLIEST=**TIME**] [LATEST=**LATEST**]
```

Examples

```
| DNSDB TARGET=203.0.113.0/24
```

```
| DNSDB TARGET="EXAMPLE.COM" LATEST=1446000216
```

DNSDBLIMIT COMMAND

Returns the DNSDB API query limit per day, the number of queries remaining today, as well as the time when the query limit will next reset.

Syntax

```
DNSDBLIMIT
```

Example

```
| DNSDBLIMIT
```

DNSDB LOOKUP

Runs dnsdb command on a set of targets.

Syntax

```
LOOKUP DNSDB [FIELDS]
```

Fields

dnsdb_host, dnsdb_ip

Example

```
... | LOOKUP DNSDB DNSDB_IP AS SRCip OUTPUT dnsdb_host_
```

TROUBLESHOOTING

PROBLEM App returns error "Authorization failed. Check API key".

CAUSE API Key is missing or incorrect.

RESOLUTION Check that your API key is entered correctly.

PROBLEM App returns error "Query limit reached".

CAUSE You have reached your query limit.

RESOLUTION Wait until your limit resets (likely at midnight daily) until making more queries.

SUPPORT AND RESOURCES

Technical support is available via email to support@farsightsecurity.com. Support requests will be responded to within 24 hours Monday through Friday.

- Hours: Monday-Friday 09:00-17:00 CST
- Observed Holidays: Major US Holidays