Network Tools - Feature #2074

Add ability to define an index to output the results to (and constrain searches to)

09/18/2017 11:17 PM - Luke Murphey

Status:	Closed	**Start date:**	09/18/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	1.2		

Description

I have a possibly unique situation in that my “customers” are given different indexes because like 2 year olds in a sandbox, they don’t play well together. So, for instance anything they contribute to Splunk, goes into their own indexes and instead of searching the main indexes for shared platforms e.g. Firewalls that data is parsed out to summary indexes that only contain traffic with a src or dest of their subnet.

I would like to offer the network toolkit to the various departments but would need to limit their access to only their interactions with it. What would be ideal is having everything a user from deptA does when interacting with the toolkit got to index_deptA. I can see a couple of ways to do this: replicate the app with different names, default index, permissions. Or use forms on the various user apps which limit the searches to their subnets.

Associated revisions

Revision 202 - 11/08/2017 06:01 AM - lukemurphey

Adding index option for outputting search command data to an index

Reference #2074

Revision 203 - 11/08/2017 07:40 AM - lukemurphey

Making it possible to declare which index to search and store the data in

Reference #2074

History

#1 - 11/08/2017 05:58 AM - Luke Murphey

To do this I need to:

Command	Command Updated	View Updated
nslookup	Yes	Yes
speedtest	Yes	Yes
whois	Yes	Yes
traceroute	Yes	Yes
ping	Yes	Yes

#2 - 11/08/2017 07:58 AM - Luke Murphey

- Status changed from New to Closed

- % Done changed from 0 to 100