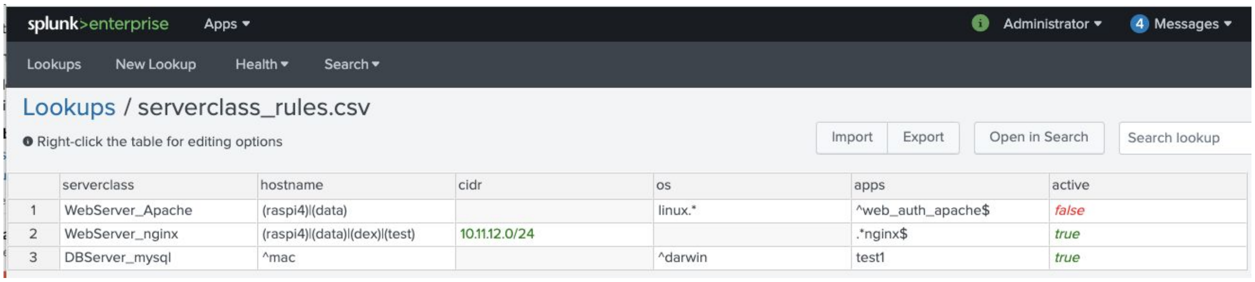
Serverclass.conf Generator App - scgen

This App is provided as-is without any warranties. It is a prototype. Feel free to enhance. And please test properly!

Usage instructions:

1) Download the app from https://github.com/bautt/scgen/blob/main/scgen.tar.gz and install on the deployment server
2) Use text editor or lookup file editor (https://splunkbase.splunk.com/app/1724/) to edit the rules file. File is deployed with the app and located in `/opt/splunk/etc/apps/scgen/lookups/serverclass_rules.csv`



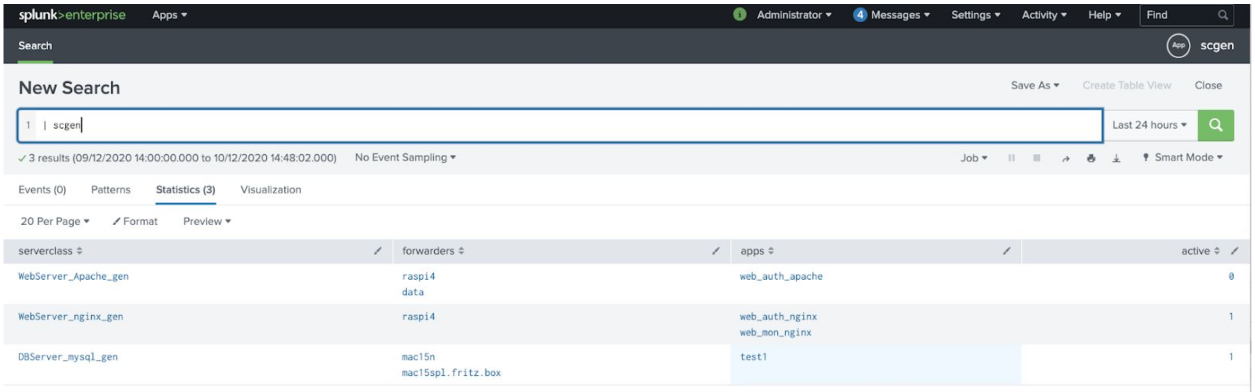
Lookups / serverclass_rules.csv

Right-click the table for editing options

<table>
<tr><th></th><th>serverclass</th><th>hostname</th><th>cidr</th><th>os</th><th>apps</th><th>active</th></tr>
<tr><td>1</td><td>WebServer_Apache</td><td>(raspi4)|(data)</td><td></td><td>linux.*</td><td>^web_auth_apache$</td><td>false</td></tr>
<tr><td>2</td><td>WebServer_nginx</td><td>(raspi4)|(data)|(dex)|(test)</td><td>10.11.12.0/24</td><td></td><td>.*nginx$</td><td>true</td></tr>
<tr><td>3</td><td>DBServer_mysql</td><td>^mac</td><td></td><td>^darwin</td><td>test1</td><td>true</td></tr>
</table>

Serverclass -> just a name for a server class
Hostname -> regex expression matching host names
CIDR -> IP range (will be used in AND with host names, both must match)
OS -> regex expression matching machine type (AND conjunction)
Apps -> regex expression matching application names (they will only appear if they exist)
Active-> boolean, if false no entry will be generated in the serverclasses conf

3) Use scgen custom search command in Splunk which will run `/opt/splunk/etc/apps/scgen/bin/scgen.py` script go through the rules and generate serverclass.conf.
   The command only exists in the context of the scgen app.



```
1 | scgen
```

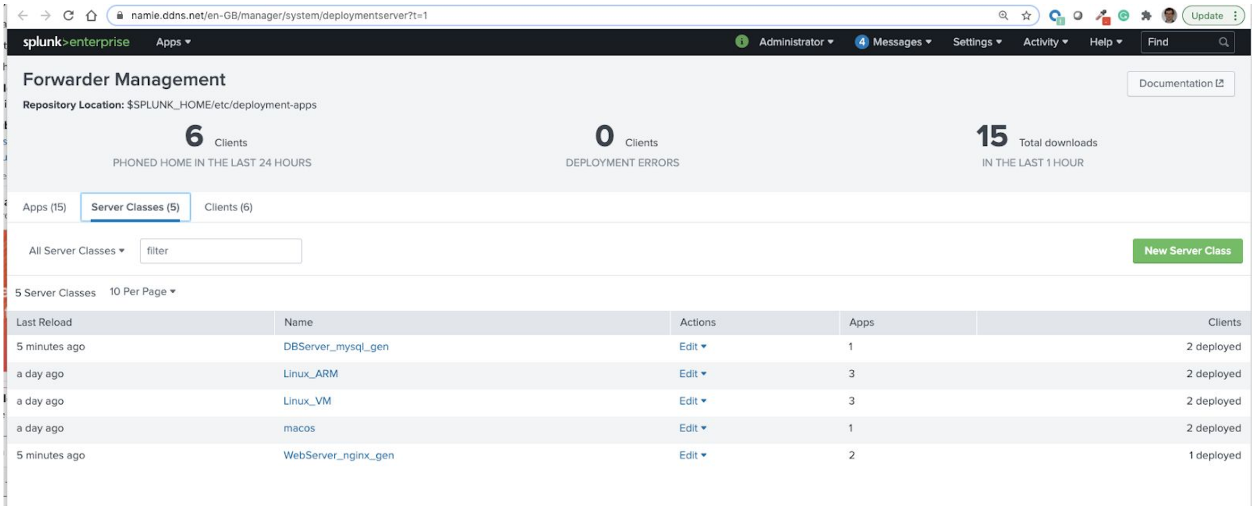
✓ 3 results (09/12/2020 14:00:00.000 to 10/12/2020 14:48:02.000)

serverclass	forwarders	apps	active
WebServer_Apache_gen	raspi4 data	web_auth_apache	0
WebServer_nginx_gen	raspi4	web_auth_nginx web_mon_nginx	1
DBServer_mysql_gen	mac15n mac15spl.fritz.box	test1	1

4) Check serverclass.conf which will be created under
`/opt/splunk/etc/apps/scgen/local/serverclass.conf`

```
[serverClass:WebServer_nginx_gen:app:web_auth_nginx]

[serverClass:WebServer_nginx_gen:app:web_mon_nginx]

[serverClass:DBServer_mysql_gen:app:test1]

[serverClass:WebServer_nginx_gen]
whitelist.0 = raspi4

[serverClass:DBServer_mysql_gen]
whitelist.0 = mac15n
whitelist.1 = mac15spl.fritz.box
```

Or check it in the UI under Settings->Forwarder Management:



Forwarder Management

Repository Location: $SPLUNK_HOME/etc/deployment-apps

6 Clients PHONED HOME IN THE LAST 24 HOURS

0 Clients DEPLOYMENT ERRORS

15 Total downloads IN THE LAST 1 HOUR

5 Server Classes

Last Reload	Name	Actions	Apps	Clients
5 minutes ago	DBServer_mysql_gen	Edit ▾	1	2 deployed
a day ago	Linux_ARM	Edit ▾	3	2 deployed
a day ago	Linux_VM	Edit ▾	3	2 deployed
a day ago	macos	Edit ▾	1	2 deployed
5 minutes ago	WebServer_nginx_gen	Edit ▾	2	1 deployed