

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`



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

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.

New Search Save As Create Table View Close

1 | scgen Last 24 hours Q

✓ 3 results (09/12/2020 14:00:00.000 to 10/12/2020 14:48:02.000) No Event Sampling

Events (0) Patterns **Statistics (3)** Visualization

20 Per Page Format Preview

serverclass	forwarders	apps	active
WebServer_apache_gen	raspi4	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) Create a scheduled search to run every minute or every X minutes. This way any new hosts matching the rules will be automatically added to the according serverclass. Same applies to the apps: any new apps, matching the the regex will be added to the assigned app list.

Edit Schedule

Report **Update Serverclasses**

This report is currently disabled.

Enable and Schedule ☒ [Learn More](#)

Schedule Run on Cron Schedule

Cron Expression ***** e.g. 00 18 *** (every day at 6PM). [Learn More](#)

Time Range Last 24 hours

Schedule Priority Default

Schedule Window No window

Trigger Actions + Add Actions

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

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

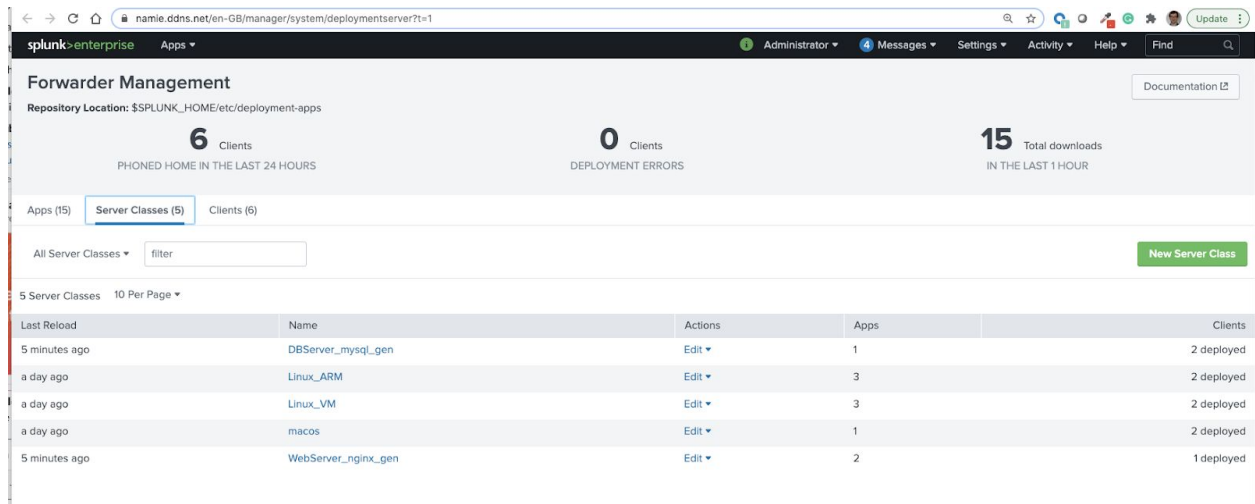
```
[serverClass:WebServer_nginx_gen:app:web_mon_nginx]
```

```
[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:



The screenshot shows the Splunk Forwarder Management interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps'. Below this, the 'Forwarder Management' section is active, showing 'Repository Location: \$SPLUNK_HOME/etc/deployment-apps'. Three summary cards are displayed: '6 Clients PHONED HOME IN THE LAST 24 HOURS', '0 Clients DEPLOYMENT ERRORS', and '15 Total downloads IN THE LAST 1 HOUR'. Below these, there are tabs for 'Apps (15)', 'Server Classes (5)', and 'Clients (6)'. The 'Server Classes (5)' tab is selected, showing a list of server classes with columns for 'Last Reload', 'Name', 'Actions', 'Apps', and 'Clients'. A 'filter' input field and a 'New Server Class' button are also visible.

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