

How to install sngrep on your VoipNow server

sngrep is a tool for displaying SIP calls message flows from the terminal of your server. It can be used to display real-time SIP traffic and to process PCAP files (packet captures). Think of it as a specialized tcpdump tool designed for VoIP. It's open-source and it's available [here](#).

This knowledge base article assumes advanced knowledge of the Linux command line and familiarity with the SIP protocol.

Step-by-step guide

Here are the steps to take if you want to install sngrep on your VoipNow server.

Please note that all commands listed in a code block need to be executed as root.

1. If VoipNow is not installed, perform the installation using the command line installer as instructed [here](#).
2. Install the required software packages so that you can download and compile sngrep by running:

```
# yum -y install git libpcap openssl-devel gnutls pcre-devel libpcap-devel ncurses-devel autoconf automake gcc make
```

3. Download the sngrep files.

```
# cd ~
# git clone https://github.com/irontec/sngrep.git
Cloning into 'sngrep'...
remote: Counting objects: 4878, done.
remote: Total 4878 (delta 0), reused 0 (delta 0), pack-reused 4878
Receiving objects: 100% (4878/4878), 4.06 MiB | 1.98 MiB/s, done.
Resolving deltas: 100% (3864/3864), done.
Checking connectivity... done.
```

4. A new folder named sngrep containing the source code will be created. Go to that folder.

```
# cd sngrep
```

5. Run the bootstrap.sh script.

```
# ./bootstrap.sh
Generating the configure script ...
```

6. Run the configure script.

```
./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports nested variables... (cached) yes
checking for style of include used by make... GNU
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking dependency style of gcc... gcc3
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for ANSI C header files... yes
```

```
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
checking for unistd.h... yes
checking minix/config.h usability... no
checking minix/config.h presence... no
checking for minix/config.h... no
checking whether it is safe to define __EXTENSIONS__... yes
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
checking dependency style of gcc... (cached) gcc3
checking for g++... no
checking for c++... no
checking for gpp... no
checking for aCC... no
checking for CC... no
checking for cxx... no
checking for cc++... no
checking for cl.exe... no
checking for FCC... no
checking for KCC... no
checking for RCC... no
checking for xlc_r... no
checking for xlc... no
checking whether we are using the GNU C++ compiler... no
checking whether g++ accepts -g... no
checking dependency style of g++... none
checking whether ln -s works... yes
checking for egrep... (cached) /usr/bin/grep -E
checking for pthread_create in -lpthread... yes
checking for pcap_open_offline in -lpcap... yes
checking pcap.h usability... yes
checking pcap.h presence... yes
checking for pcap.h... yes
checking ncurses.h usability... yes
checking ncurses.h presence... yes
checking for ncurses.h... yes
checking for initscr in -lncurses... yes
checking for new_panel in -lpanel... yes
checking for new_form in -lform... yes
checking for new_item in -lmenu... yes
```

configure:

configure: sngrep configure finished

configure: =====

configure: GnuTLS Support : no

configure: OpenSSL Support : no

configure: Unicode Support : no

configure: Perl Expressions Support : no

configure: IPv6 Support : no

configure: EEP Support : no

configure: =====

configure:

checking that generated files are newer than configure... done

configure: creating ./config.status

config.status: creating Makefile

config.status: creating src/Makefile

config.status: creating config/Makefile

config.status: creating doc/Makefile

```
config.status: creating tests/Makefile
config.status: creating src/config.h
config.status: executing depfiles commands
```

7. Compile sngrep with the make command.

```
# make
Making all in src
make[1]: Entering directory `/root/sngrep/src'
make all-am
make[2]: Entering directory `/root/sngrep/src'
CC      capture.o
CC      address.o
CC      packet.o
CC      sip.o
CC      sip_call.o
CC      sip_msg.o
CC      sip_attr.o
CC      main.o
CC      option.o
CC      group.o
CC      filter.o
CC      keybinding.o
CC      media.o
CC      setting.o
CC      rtp.o
CC      util.o
CC      vector.o
CC      ui_panel.o
CC      scrollbar.o
CC      ui_manager.o
CC      ui_call_list.o
CC      ui_call_flow.o
CC      ui_call_raw.o
CC      ui_stats.o
CC      ui_filter.o
CC      ui_save.o
CC      ui_msg_diff.o
CC      ui_column_select.o
CC      ui_settings.o
CCLD    sngrep
make[2]: Leaving directory `/root/sngrep/src'
make[1]: Leaving directory `/root/sngrep/src'
Making all in config
make[1]: Entering directory `/root/sngrep/config'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/root/sngrep/config'
Making all in doc
make[1]: Entering directory `/root/sngrep/doc'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/root/sngrep/doc'
Making all in tests
make[1]: Entering directory `/root/sngrep/tests'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/root/sngrep/tests'
make[1]: Entering directory `/root/sngrep'
make[1]: Nothing to be done for `all-am'.
make[1]: Leaving directory `/root/sngrep'
```

8. Install sngrep with the make install command.

```
# make install
Making install in src
make[1]: Entering directory `/root/sngrep/src'
make[2]: Entering directory `/root/sngrep/src'
  /usr/bin/mkdir -p '/usr/local/bin'
  /usr/bin/install -c sngrep '/usr/local/bin'
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/root/sngrep/src'
make[1]: Leaving directory `/root/sngrep/src'
Making install in config
make[1]: Entering directory `/root/sngrep/config'
make[2]: Entering directory `/root/sngrep/config'
  /usr/bin/mkdir -p '/usr/local/etc'
  /usr/bin/install -c -m 644 sngrepc '/usr/local/etc'
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/root/sngrep/config'
make[1]: Leaving directory `/root/sngrep/config'
Making install in doc
make[1]: Entering directory `/root/sngrep/doc'
make[2]: Entering directory `/root/sngrep/doc'
make[2]: Nothing to be done for `install-exec-am'.
  /usr/bin/mkdir -p '/usr/local/share/man/man8'
  /usr/bin/install -c -m 644 sngrep.8 '/usr/local/share/man/man8'
make[2]: Leaving directory `/root/sngrep/doc'
make[1]: Leaving directory `/root/sngrep/doc'
Making install in tests
make[1]: Entering directory `/root/sngrep/tests'
make[2]: Entering directory `/root/sngrep/tests'
make[2]: Nothing to be done for `install-exec-am'.
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/root/sngrep/tests'
make[1]: Leaving directory `/root/sngrep/tests'
make[1]: Entering directory `/root/sngrep'
make[2]: Entering directory `/root/sngrep'
make[2]: Nothing to be done for `install-exec-am'.
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/root/sngrep'
make[1]: Leaving directory `/root/sngrep'
```

9. sngrep is now installed into /usr/local/bin/sngrep which should be already in your path. You may launch it with the sngrep command:

```
# sngrep
```

After starting sngrep, you'll be presented with a text-mode, interactive interface which can be navigated with the arrow keys and quit with the Esc key.

How to make the most of SNGREP

Initialize a softphone which registers to your VoipNow server, and the REGISTER and the SUBSCRIBE methods sent by the phone will appear in the console right away. You can clear the list of captured messages by pressing the F5 key, as indicated in the legend at the bottom of the screen.

sngrep - SIP messages flow viewer							
Current Mode: Online		Dialogs: 2					
Display Filter:							
	Method	SIP From	SIP To	Msgs	Source	Destination	Call State
[] 1	REGISTER	0003*002@10.150.8.21:5060	0003*002@10.150.8.21:5060	4	192.168.3.189:56712	10.150.8.21:5060	
[] 2	SUBSCRIBE	0003*002@10.150.8.21:5060	0003*002@10.150.8.21:5060	4	192.168.3.189:56712	10.150.8.21:5060	

You can move the cursor between the displayed packets using the arrow keys. For details about a specific SIP method, press ENTER. You'll get a graphical flow of the packets exchanged between your phone and the VoipNow server. You may navigate through the flow using the same arrow keys - the selected message details will be displayed on the right of the window.

Call flow for NtnhMTAGYsY2ZWQzOthhNtg2MWeyNtVKMjEz2YsZWE. (Color by Request/Response)		
192.168.3.189:56712	10.150.8.21:5060	REGISTER sip:10.150.8.21:5060 SIP/2.0
		Via: SIP/2.0/UDP 192.168.3.189:56712;branch=z9hG4bK-d8754z-b42c2d6ac977f91c-1--d8754z-rport
		Max-Forwards: 70
		Contact: <sip:0003*0028192.168.3.189:56712;rinstance=1clbf515683da4b4>
12:34:16.463983	REGISTER	To: "4PSATEST"<sip:0003*002810.150.8.21:5060>
+0.001068	401 Unauthorized	From: "4PSATEST"<sip:0003*002810.150.8.21:5060>;tag=0a390a23
12:34:16.465051	401 Unauthorized	Call-ID: NtnhMTAGYsY2ZWQzOthhNtg2MWeyNtVKMjEz2YsZWE
+0.102470	REGISTER	CSseq: 1 REGISTER
12:34:16.567521	REGISTER	Expires: 120
+0.005218	200 OK	Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE
12:34:16.592799	200 OK	Supported: replace
+108.1341785	REGISTER	User-Agent: 3CXPhone 6.0.0.26523.0
12:36:04.714528	REGISTER	Content-Length: 0
+0.001707	401 Unauthorized	X-Do: PHPpcDowMDazFjAwkKxOTlMty4LjMlMtg5QzU2NzEzO3JpbN0YW5kZjTOXzFzFjZlXkNtYzRmRnIG0Pq==
12:36:04.716235	401 Unauthorized	X-Dv: U0lQLzUwC3VRFAgMTkyYjE2OC4LzEjE4OT0tMjYjcmxjZi1cmFuZUy2g9ejloRzRlSjYlK0dCNH0tYjQyYzY0LzU0ZDg3NTR6LlRyYyG9yda==
+0.103391	REGISTER	
12:36:04.819626	REGISTER	
+0.006560	200 OK	
12:36:04.826486	200 OK	

```
2016/05/13 12:34:16.463983 192.168.3.189:56712 -> 10.150.8.21:5060
REGISTER sip:10.150.8.21:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.3.189:56712;branch=z9hG4bK-d8754z-b42c2d6ac977f91c-1---d8754z;rport
Max-Forwards: 70
Contact: <sip:0003*002@192.168.3.189:56712;rinstance=1clbf515683da4b4>
To: "4PSATEST"<sip:0003*002@10.150.8.21:5060>
From: "4PSATEST"<sip:0003*002@10.150.8.21:5060>;tag=0a390a23
Call-ID: NthlMTA0YjY2ZWQzOThhNTg2MWEyNTVhK4jEzM2Y5ZWU.
CSeq: 1 REGISTER
Expires: 120
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE
Supported: replaces
User-Agent: 3CXPhone 6.0.26523.0
Content-Length: 0
X-De: PHNpcDowMDAzKjAwMkAxOTUuMTY4LjIjMuMTg5OjU2NzEyO3JpbmN0YW5jZT0xYzFiZjUxNTY4M2RmNGI0Pg==
X-Dv: U0lQLZlUuMCM9VRFAgMtkYjLE2OC4zLjE4OT0iNjcxMjticmFuY2g9ejJlRzRiSylkODc1NH0tYjYyYzJkNmFjOTc3ZjkyY0xLS0tZDg3NTR6LTtYcG9ydA==
```

1. The initial REGISTER sent by the phone (informing the server of his presence).

2. The 401 Unauthorized sent by the server to the phone (containing the challenge to which the phone has to reply).

3. The second REGISTER message sent by the phone (with the valid credentials, user ID and password).

4. The 200 OK confirming the phone has registered correctly with the server.

call flow for MHAHAADVY2ZHQGQTHaHTg2HWEjHTVWVjKMGJGYZNW. (Color by Request/Response)		
192.160.3.189:56712	10.150.8.21:5060	[STP/2.0 401 Unauthorized Via: SIP/2.0/UDP 192.160.3.189:56712;branch=branch048--d875a3-b42d8d6c577f91c1--d875a3-report-56712 To: <[CONTACT]*sip:0003@002810.150.8.21>[6040];tag=3054080b1f9c3b370da1a1b2df72-6e49 From: <MFASTATEST*sip:0003@002810.150.8.21>[5060];tag=0a390a23 Call-ID: HTLMTAVY2ZHQGQTHaHTg2HWEjHTVWVjKMGJGYZNW. Contact: 3 REGISTER WWW-Authenticate: Digest realm="10.150.8.21", nonce="VxK51c1cydjdIpI9/8xk5U8ghvWgWd" Server: VoipNow PBX Content-Length: 0
12:34:16.463993	401 Unauthorized	
12:34:16.465051	401 Unauthorized	
12:34:16.467021	200 OK	
12:34:16.467218	200 OK	
12:34:16.472739	401 Unauthorized	
12:34:16.473128	401 Unauthorized	
12:34:16.474225	200 OK	
12:34:16.474696	200 OK	
12:34:16.475739	401 Unauthorized	
12:34:16.476238	401 Unauthorized	
12:34:16.476696	200 OK	
12:34:16.477143	200 OK	
12:34:16.477599	401 Unauthorized	
12:34:16.478058	401 Unauthorized	
12:34:16.478516	200 OK	
12:34:16.478974	200 OK	
12:34:16.479432	200 OK	
12:34:16.479890	200 OK	
12:34:16.480348	200 OK	
12:34:16.480806	200 OK	
12:34:16.481264	200 OK	
12:34:16.481722	200 OK	
12:34:16.482180	200 OK	
12:34:16.482638	200 OK	
12:34:16.483096	200 OK	
12:34:16.483554	200 OK	
12:34:16.484012	200 OK	
12:34:16.484470	200 OK	
12:34:16.484928	200 OK	
12:34:16.485386	200 OK	
12:34:16.485844	200 OK	
12:34:16.486302	200 OK	
12:34:16.486760	200 OK	
12:34:16.487218	200 OK	
12:34:16.487676	200 OK	
12:34:16.488134	200 OK	
12:34:16.488592	200 OK	
12:34:16.489050	200 OK	

Place a call to *52 (the echo test) and you'll see the call appear in the list.

Pressing ENTER will open a call flow diagram illustrating the communication between the phone and the SIP/PBX components of VoipNow.

sngrep - SIP messages flow viewer						
Current Mode: Online		Dialogs: 1				
Display Filter:						
	Msg Method	SIP From	SIP To	Msgs	Source	Destination
[] 1	INVITE	0003*002@10.150.8.21:5060	*52@10.150.8.21:5060	16	192.168.3.189:56712	10.150.8.21:5060
						IN CALL

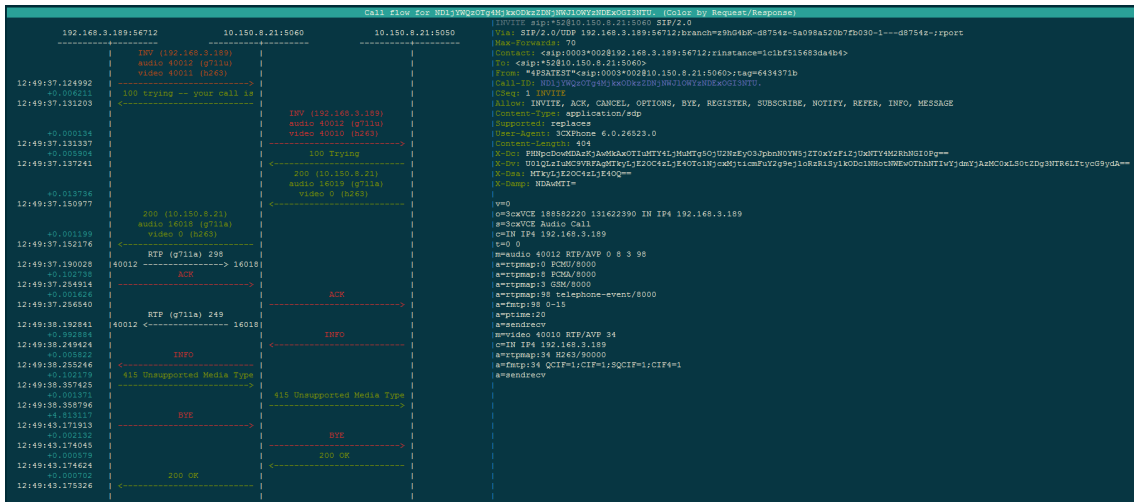
[illegible]

More great SNGREP features

For example, you can compare two SIP packets by checking them with the Space key. Once the second packet is checked, the differences between the two packets will be automatically shown in a separate window.

	shrip - SIP message flow viewer
2016/05/13 12:50:30.774908 192.168.3.189:56712 --> 10.150.8.21:5060	2016/05/13 12:50:30.877033 192.168.3.189:56712 --> 10.150.8.21:5060
REGISTER sip:10.150.8.21:5060 SIP/2.0	REGISTER sip:10.150.8.21:5060 SIP/2.0
To: *WSATSTZ/cap10003@0028192.168.3.189:56712;branch=9HG4Bk-dt754e-2c23931131647E451r---d8754e;-rport	To: *WSATSTZ/cap10003@0028192.168.3.189:56712;branch=9HG4Bk-dt754e-493e83156972bf5f1r---d8754e;-rport
Max-Forwards: 70	Max-Forwards: 70
Contact: <cap10003@0028192.168.3.189:56712;rinstance=1clbf515683da4b>	Contact: <cap10003@0028192.168.3.189:56712;rinstance=1clbf515683da4b>
From: *WSATSTZ/cap10003@0028192.168.3.189:56712	From: *WSATSTZ/cap10003@0028192.168.3.189:56712
To: *WSATSTZ/cap10003@0028192.168.3.189:56712	To: *WSATSTZ/cap10003@0028192.168.3.189:56712
Call-ID: NTHlMTAOyYzZWQzOThhMtG2MWEyHTVMXEMzYSZW.	Call-ID: NTHlMTAOyYzZWQzOThhMtG2MWEyHTVMXEMzYSZW.
Sseq: 20 REGISTER	Sseq: 20 REGISTER
Expires: 120	Expires: 120
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE	Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE
Supported: replaces	Supported: replaces
User-Agent: 3CXPhone 6.0.26523.0	User-Agent: 3CXPhone 6.0.26523.0
Content-Length: 0	Content-Length: 0
A-Digest: SHA256UWVwH43Ahdv0tUfT43JmHnG0Sv9U93j3pbNq0W5IzRxfzFzDxTWT4M2BhH0IG==	A-Digest: HBBpCooDv0d3K4MdnKA0WtL4H14LH4p0W93j3pbNq0W5IzRxfzFzDxTWT4M2BhH0IG==
X-CSeq: 1016314163-3VR8qAFgYKt3J20C4F1K40TL0W-SMG1cmzWz2ge31o6zPisyl10Dcn1MotNmMlysktMtlMYOOCOWSdX1SotZd3NTNR	X-CSeq: 1016314163-3VR8qAFgYKt3J20C4F1K40TL0W-SMG1cmzWz2ge31o6zPisyl10Dcn1MotNmMlysktMtlMYOOCOWSdX1SotZd3NTNR
LTrtyd3ymd==	LTrtyd3ymd==

If you press F2 and F3 in a call flow, you will be able to see SDP and RTP information.



There are more options and features in sngrep, so feel free to explore further. While a bit more cumbersome to use than Wireshark, sngrep can help you quickly debug SIP problems on your server.

Related articles

- [How to install sngrep on your VoipNow server](#)
- [Primary and secondary server setup for 4PSA DNS Manager](#)
- [How to interact with RabbitMQ](#)
- [How to Allow 4PSA Access to the Server](#)
- [How to do a data migration between two DNSManager servers](#)