TACACS+ for user Authentication/Accounting/Authorization

TACACS+ (Terminal Access Controller Access-Control System Plus) is an authentication protocol that allows a remote access server to forward a login password for a user to an authentication server to determine whether access is allowed to a given system. In addition to the authentication service, TACACS+ can also provide authorization and accounting services.
TACACS for Authentication
TACACS for Accounting
TACACS for Authorization

Restriction:
If the user sets the authentication priority "local" and then to "tacacs+", the user must retry with the TACACS + account three times. Users can add "fallthrough" to avoid this behavior.
admin@sonic:~$ sudo config aaa authentication failthrough enable
Before 202111.0, AAA only supports authentication.
After 202111.0 or later, AAA supports authentication, authorization, and accounting.
Known issue: In tacacs+ environment, you will face the following warning message when you run command by sudo group.(This issue is fixed in 202006.1)
admin@sonic:~$ sudo su
usermod: Permission denied.
usermod: cannot lock /etc/passwd; try again later.
usermod: Permission denied.
Default Setting:
Before 202111.0

admin@sonic:~$ show tacacs
TACPLUS global auth_type pap (default)
TACPLUS global timeout 5 (default)
TACPLUS global passkey (default)

admin@sonic:~$ show aaa
AAA authentication login local (default)
AAA authentication failthrough False (default)
After 202111.0 or later.

admin@sonic:~$ show tacacs
TACPLUS global auth_type pap (default)
TACPLUS global timeout 5 (default)
TACPLUS global passkey <EMPTY_STRING> (default)

admin@sonic:~$ show aaa
AAA authentication login local (default)
AAA authentication failthrough False (default)
AAA authorization login local (default)
AAA accounting login disable (default)

TACACS for Authentication
Topology:
mceclip0.png

Procedure:

Step 1. Set the management IP on the switch ([Edgecore SONiC] Management and front port IPv4/IPv6 Address)

Step 2: Add the TACACS Server host to the switch

admin@sonic:~$ sudo config tacacs add 188.188.87.101
Step 3: Set the TACACS authentication key (support as an example)

```
admin@sonic:~$ sudo config tacacs passkey support
Step 4: Use tacacs+ database for user authentication

admin@sonic:~$ sudo config aaa authentication login local tacacs+
Note: Since the restriction, once the authentication priority of the "local" is
higher than "tacacs+", Users may enable "fallthrough".

admin@sonic:~$ sudo config aaa authentication failthrough enable

Result:
Check the TACACS server settings (Below the show command is for version
202111.0)
admin@sonic:~$ show tacacs
TACPLUS global auth_type pap (default)
TACPLUS global timeout 5 (default)
TACPLUS global passkey ******

TACPLUS_SERVER address 188.188.87.101
               priority 1
               tcp_port 49
Check aaa settings.  (Below the show command is for version 202111.0)

admin@sonic:~$ show aaa
AAA authentication login local,tacacs+
AAA authentication failthrough True
AAA authorization login local (default)
AAA accounting login disable (default)
Login with the tacacs+ account.
1. Login via console:

Debian GNU/Linux 11 sonic ttyS0

sonic login: gavin1
Password:
Linux sonic 5.10.0-8-2-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64
You are on
  ____   ___  _   _ _  ____
/ ___| / _ \| \ | (_)/ ___|
\___ \| | | |  \| | | |
  ___) | |_| | |\  | | |___
|____/ \___/|_| \_|_|\____|

-- Software for Open Networking in the Cloud --

Unauthorized access and/or use are prohibited.
All access and/or use are subject to monitoring.

Help:    http://azure.github.io/SONiC/

gavin1@sonic:~$

2. Login via SSH:

gavin@gavindeMacBook-Air ~ % ssh gavin1@188.188.97.6
gavin1@188.188.97.6's password:
Linux sonic 5.10.0-8-2-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64
You are on
  ____   ___  _   _ _  ____
/ ___| / _ \| \ | (_)/ ___|
\___ \| | | |  \| | | |
  ___) | |_| | |\  | | |___
|____/ \___/|_| \_|_|\____|

-- Software for Open Networking in the Cloud --
```

```
Unauthorized access and/or use are prohibited.
All access and/or use are subject to monitoring.

Help:    http://azure.github.io/SONiC/

Last login: Sun Mar 27 20:12:27 2022
gavin1@sonic:~$
Appendix:
TACACS+ server configuration:
TACACS_SERVER# cat /etc/tacacas+/tac_plus.cfg
key = support
user = gavin15 {
    default service = permit
    pap = cleartext "gavin15"
    service = exec {
                priv-lvl = 15
            }
}
user = gavin1 {
    default service = permit
    pap = cleartext "gavin1"
    service = exec {
                priv-lvl = 1
        }
}


TACACS for Accounting
Procedure:

Step 1:  Enable the TACACS+ Authentication  (Refer to the TACACS for
Authentication )

Step 2:  Enable the TACACS+ accounting.

admin@sonic:~$ sudo config aaa accounting tacacs+
Result:

Check aaa settings.  (Below the show command is for version 202111.0)

admin@sonic:~$ show aaa
AAA authentication login local,tacacs+
AAA authentication failthrough True
AAA authorization login local (default)
AAA accounting login tacacs+
Check the log on TACACS Server. (Below is the log for "show vlan brief")

Jul  1 08:29:31    188.188.97.6    gavin15    pts1    sonic    stop
start_time=1656692957    task_id=9339    service=    cmd=/usr/bin/python3.9
exit=1
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9403    service=    cmd=/usr/bin/python3.9
/usr/local/bin/show vlan brief
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9404    service=    cmd=/usr/bin/python3.9
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9404    service=    cmd=/usr/bin/uname -p
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    stop
start_time=1656692957    task_id=9404    service=    cmd=/usr/bin/uname exit=0
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9405    service=    cmd=/usr/bin/python3.9
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9405    service=    cmd=/usr/bin/file -b
```

```
/usr/bin/python3.9
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    stop
start_time=1656692957    task_id=9405    service=    cmd=/usr/bin/file exit=0
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9406    service=    cmd=/usr/bin/dash -c sudo
docker ps | grep bgp | awk '{print$2}' | cut -d'-' -f3 | cut -d':' -f1 | head -n
1
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9407    service=    cmd=/usr/bin/sudo docker ps
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9408    service=    cmd=/usr/bin/grep bgp
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9410    service=    cmd=/usr/bin/cut -d- -f3
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9409    service=    cmd=/usr/bin/mawk {print$2}
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9411    service=    cmd=/usr/bin/cut -d: -f1
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9412    service=    cmd=/usr/bin/head -n 1
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    start
start_time=1656692957    task_id=9413    service=    cmd=/usr/bin/docker ps
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    stop
start_time=1656692957    task_id=9413    service=    cmd=/usr/bin/docker exit=0
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    stop
start_time=1656692958    task_id=9407    service=    cmd=/usr/bin/sudo exit=0
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    stop
start_time=1656692958    task_id=9408    service=    cmd=/usr/bin/grep exit=0
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    stop
start_time=1656692958    task_id=9409    service=    cmd=/usr/bin/mawk exit=0
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    stop
start_time=1656692958    task_id=9410    service=    cmd=/usr/bin/cut exit=0
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    stop
start_time=1656692958    task_id=9411    service=    cmd=/usr/bin/cut exit=0
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    stop
start_time=1656692958    task_id=9412    service=    cmd=/usr/bin/head exit=0
Jul  1 08:29:32    188.188.97.6    gavin15    pts1    sonic    stop
start_time=1656692958    task_id=9406    service=    cmd=/usr/bin/dash exit=0
Appendix:
TACACS+ server configuration:
TACACS_SERVER# cat /etc/tacacas+/tac_plus.cfg
accounting file = /var/log/tac_plus.acct
key = support
user = gavin15 {
    default service = permit
    pap = cleartext "gavin15"
    service = exec {
                priv-lvl = 15
            }
}
user = gavin1 {
    default service = permit
    pap = cleartext "gavin1"
    service = exec {
                priv-lvl = 1
        }
}


TACACS for Authorization
Procedure:

Step 1:  Enable the TACACS+ Authentication  (Refer to the TACACS for
Authentication )
```

Step 2: Enable the TACACS+ Authorization.

```
admin@sonic:~$ sudo config aaa authorization tacacs+
Result:

Check aaa settings.  (Below the show command is for version 202111.0)

admin@sonic:~$ show aaa
AAA authentication login local,tacacs+
AAA authentication failthrough True
AAA authorization login tacacs+
AAA accounting login tacacs+
Using the privilege 15 of the account, it will be got "sudo" permission.

Debian GNU/Linux 11 sonic ttyS0

sonic login: gavin15
Password:
Linux sonic 5.10.0-8-2-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64
You are on
  ____   ___  _   _ _  ____
/ ___| / _ \| \ | (_)/ ___|
\___ \| | | |  \| | | |
  ___) | |_| | |\  | | |___
|____/ \___/|_| \_|_|\____|

-- Software for Open Networking in the Cloud --

Unauthorized access and/or use are prohibited.
All access and/or use are subject to monitoring.

Help:    http://azure.github.io/SONiC/

Last login: Sun Mar 27 20:51:46 UTC 2022 on ttyS0
gavin15@sonic:~$ id
uid=1003(gavin15) gid=1000(admin) groups=1000(admin),27(sudo),999(docker)
gavin15@sonic:~$


Using privilege 1 of the account, and this account only be authorized to use the
"show version", other commands are not allowed.

Debian GNU/Linux 11 sonic ttyS0

sonic login: gavin1
Password:
Linux sonic 5.10.0-8-2-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64
You are on
  ____   ___  _   _ _  ____
/ ___| / _ \| \ | (_)/ ___|
\___ \| | | |  \| | | |
  ___) | |_| | |\  | | |___
|____/ \___/|_| \_|_|\____|

-- Software for Open Networking in the Cloud --

Unauthorized access and/or use are prohibited.
All access and/or use are subject to monitoring.

Help:    http://azure.github.io/SONiC/

Last login: Sun Mar 27 20:55:51 UTC 2022 on ttyS0
gavin1@sonic:~$ id
uid=1004(gavin1) gid=100(users) groups=100(users)
```

```
gavin1@sonic:~$ show ip interface
/usr/local/bin/show authorize failed by TACACS+ with given arguments, not
executing


gavin1@sonic:~$ show version

SONiC Software Version: SONiC.Edgecore-SONiC_20220526_081320_ec202111_117
Distribution: Debian 11.3
Kernel: 5.10.0-8-2-amd64
Build commit: bbb15c936
Build date: Thu May 26 09:40:32 UTC 2022
Built by: ubuntu@ip-10-5-1-178

Platform: x86_64-accton_as5835_54t-r0
HwSKU: Accton-AS5835-54T
ASIC: broadcom
ASIC Count: 1
Serial Number: 583554T1922012
Model Number: FP1ZZ56540B0A
Hardware Revision: N/A
Uptime: 15:10:09 up 42 min,  2 users,  load average: 1.52, 1.42, 1.33

Docker images:
REPOSITORY                  TAG
IMAGE ID       SIZE
docker-teamd                Edgecore-SONiC_20220526_081320_ec202111_117
3033477188fd   442MB
docker-teamd                latest
3033477188fd   442MB
docker-syncd-brcm           Edgecore-SONiC_20220526_081320_ec202111_117
953c477d3061   630MB
docker-syncd-brcm           latest
953c477d3061   630MB
docker-stp                  Edgecore-SONiC_20220526_081320_ec202111_117
a65998a7d50e   458MB
docker-stp                  latest
a65998a7d50e   458MB
docker-sflow                Edgecore-SONiC_20220526_081320_ec202111_117
5b5ab66df377   443MB
docker-sflow                latest
5b5ab66df377   443MB
docker-orchagent            Edgecore-SONiC_20220526_081320_ec202111_117
06e4550c6cf6   464MB
docker-orchagent            latest
06e4550c6cf6   464MB
docker-nat                  Edgecore-SONiC_20220526_081320_ec202111_117
a24548f15e96   445MB
docker-nat                  latest
a24548f15e96   445MB
docker-macsec               Edgecore-SONiC_20220526_081320_ec202111_117
d67f8d7d21aa   445MB
docker-macsec               latest
d67f8d7d21aa   445MB
docker-iccpd                Edgecore-SONiC_20220526_081320_ec202111_117
744fe73aeac2   446MB
docker-iccpd                latest
744fe73aeac2   446MB
docker-fpm-frr              Edgecore-SONiC_20220526_081320_ec202111_117
a06281b8f1d4   471MB
docker-fpm-frr              latest
a06281b8f1d4   471MB
```

```
docker-lldp                   Edgecore-SONiC_20220526_081320_ec202111_117
baa2863959da   468MB
docker-lldp                   latest
baa2863959da   468MB
docker-platform-monitor       Edgecore-SONiC_20220526_081320_ec202111_117
71b3360a58cf   694MB
docker-platform-monitor       latest
71b3360a58cf   694MB
docker-sonic-mgmt-framework   Edgecore-SONiC_20220526_081320_ec202111_117
1de640e23ebb   706MB
docker-sonic-mgmt-framework   latest
1de640e23ebb   706MB
docker-sonic-telemetry        Edgecore-SONiC_20220526_081320_ec202111_117
e5516c6c2896   514MB
docker-sonic-telemetry        latest
e5516c6c2896   514MB
docker-sonic-p4rt             Edgecore-SONiC_20220526_081320_ec202111_117
f623260fd050   523MB
docker-sonic-p4rt             latest
f623260fd050   523MB
docker-dhcp-relay             latest
3bd6b85e6bbd   440MB
docker-snmp                   Edgecore-SONiC_20220526_081320_ec202111_117
58a61cfd9e52   471MB
docker-snmp                   latest
58a61cfd9e52   471MB
docker-mux                    Edgecore-SONiC_20220526_081320_ec202111_117
faa9e2c3d9ca   479MB
docker-mux                    latest
faa9e2c3d9ca   479MB
docker-gbsyncd-credo          Edgecore-SONiC_20220526_081320_ec202111_117
ea1772f85bfe   481MB
docker-gbsyncd-credo          latest
ea1772f85bfe   481MB
docker-database               Edgecore-SONiC_20220526_081320_ec202111_117
ac797e36b0ed   427MB
docker-database               latest
ac797e36b0ed   427MB
docker-router-advertiser      Edgecore-SONiC_20220526_081320_ec202111_117
9ef8ce9d34f0   427MB
docker-router-advertiser      latest
9ef8ce9d34f0   427MB
k8s.gcr.io/pause              3.4.1
0f8457a4c2ec   683kB

gavin1@sonic:~$
Appendix:
TACACS+ server configuration:
TACACS_SERVER# cat /etc/tacacas+/tac_plus.cfg
accounting file = /var/log/tac_plus.acct
key = support
user = gavin15 {
    default service = permit
    pap = cleartext "gavin15"
    service = exec {
                priv-lvl = 15
            }
}
user = gavin1 {
    default service = permit
    pap = cleartext "gavin1"
    service = exec {
                priv-lvl = 1
        }
```

```
    cmd = /usr/local/bin/show {
        permit version
        deny
    }
}
```