使用EAA+NQA实现客户需求：当Radius服务器宕机时即使不安装802.1X客户端的终端也能实现逃

802.1X Radius **程咪** 2019-10-30 发表

问题描述

使用EAA+NQA实现客户需求：当Radius服务器宕机时即使不安装802.1X客户端的终端也能实现逃

解决方法

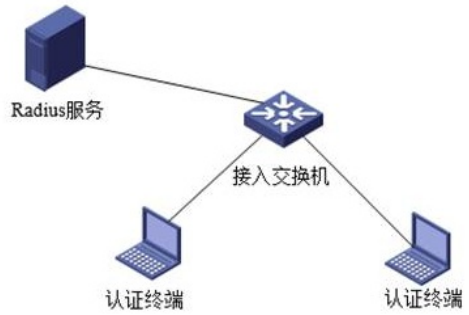
客户需求：

现场部署S5130-52S-EI结合第三方Radius服务器对终端做802.1X认证，在实施中客户提出：当Radius服务器宕机时，不管下联终端是否安装了802.1X客户端都能实现逃生的需求。

需求分析：

Radius服务器宕机时安装802.1X客户端的终端实现逃生，实现方式有很多：比如802.1X逃生、在Domain添加radius方案时后面加None做备份、Critical VLAN等都能实现，但是未安装802.1X客户端的电脑连1X 认证请求（EAPOL-Start）都不发，后续的逃生也无从谈起，只能顺着Radius服务器宕机后怎么能让接口1X认证失效来实现此需求。

测试组网：



测试步骤：

1、 配置802.1X认证

```
#
dot1x
dot1x authentication-method eap
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 999
dot1x
#
radius scheme liu
primary authentication 1.1.1.2
primary accounting 1.1.1.2
key authentication cipher $c$3$kZb+amFjQF76D6SkkdqrUfr1qZHNJQ==
key accounting cipher $c$3$KpRfo9L/08MRHJG1VV9zmgsFHRKs/g==
user-name-format without-domain
#
domain system
authentication lan-access radius-scheme liu
authorization lan-access radius-scheme liu
accounting lan-access radius-scheme liu
#
domain default enable system
```

2、 开启EAA+NQA联动

```
#
nqa entry 1 1
type icmp-echo
 destination ip 1.1.1.2   \\监控radius服务器地址
 frequency 1000
 probe timeout 100
 reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
#
```

nqa schedule 1 1 start-time now lifetime forever
#
track 1 nqa entry 1 1 reaction 1
#
[H3C]display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 3 minutes 5 seconds
  Tracked object type: NQA
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: 1 1
    Reaction: 1
    Remote IP/URL: 1.1.1.2
    Local IP: --
Interface: --
    创建EAA策略1，当track联动为negative时执行undo dot1x命令。
#
rtm cli-policy 1
event track 1 state negative
action 0 cli system
action 1 cli undo dot1x
commit
创建EAA策略2，当track联动为positive时执行dot1x命令。
rtm cli-policy 2
event track 1 state positive
action 0 cli system
action 1 cli dot1x
3、 Radius服务器宕机测试
[H3C-GigabitEthernet0/4]shutdown \\将连接服务器端口关闭
[H3C-GigabitEthernet0/4]%Jan 1 00:27:49:600 2011 H3C IFNET/3/PHY_UPDOWN: Physical state o
n the interface GigabitEthernet0/4 changed to down.
%Jan 1 00:27:49:601 2011 H3C IFNET/5/LINK_UPDOWN: Line protocol state on the interface Gigab
itEthernet0/4 changed to down.
*Jan 1 00:27:49:756 2011 H3C NQA/7/Event: NQA entry (1-1): Probe timed out.
*Jan 1 00:27:50:756 2011 H3C NQA/7/Event: NQA entry (1-1): Probe timed out.
*Jan 1 00:27:51:756 2011 H3C NQA/7/Event: NQA entry (1-1): Probe timed out.
%Jan 1 00:27:51:756 2011 H3C NQA/6/NQA_ENTRY_PROBE_RESULT: Reaction entry 1 of NQA e
ntry admin-name 1 operation-tag 1: probe-fail.
*Jan 1 00:27:51:756 2011 H3C NQA/7/Reaction: NQA entry (1-1) reaction (1): Status changed from b
elow-threshold to over-threshold.
*Jan 1 00:27:51:756 2011 H3C NQA/7/Reaction: NQA entry (1-1) reaction (1): Trigger notified.
*Jan 1 00:27:51:757 2011 H3C TRACK/7/Debug: Received the notification that the state of NQA (1-1
) reaction (1) had changed to over-threshold.
*Jan 1 00:27:51:757 2011 H3C TRACK/7/Debug: The state of track entry 1 changed from Positive to
Negative.
*Jan 1 00:27:51:758 2011 H3C TRACK/7/Debug: Track 1 status has changed, try to notify policy 1, e
ventkey 0, suppress time 0, last trigger time 0.
%Jan 1 00:27:51:868 2011 H3C DOT1X/6/DOT1X_LOGOFF: -IfName=GigabitEthernet0/6-MACAddr
=c454-4481-36c5-VLANId=1-UserName=aaa-ErrCode=5; Session of the 802.1X user was terminated
.
%Jan 1 00:27:51:889 2011 H3C RTM/6/RTM_POLICY: **CLI policy 1 is running successfully.**
dis cu
#
version 7.1.064, Release 0615P11
#
sysname H3C
#
dot1x authentication-method eap \\命令已经删除
#
4、服务器恢复测试
di%Jan 1 00:28:34:065 2011 H3C IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitE
thernet0/4 changed to up.
%Jan 1 00:28:34:065 2011 H3C IFNET/5/LINK_UPDOWN: Line protocol state on the interface Gigab

itEthernet0/4 changed to up.
#
interface GigabitEthernet0/4
port link-mode bridge
#
return
[H3C-GigabitEthernet0/4]*Jan 1 00:28:34:766 2011 H3C NQA/7/Event: NQA entry (1-1): Probe timed out.

*Jan 1 00:28:35:766 2011 H3C NQA/7/Event: NQA entry (1-1): Probe timed out.

*Jan 1 00:28:36:766 2011 H3C NQA/7/Event: NQA entry (1-1): Probe timed out.

%Jan 1 00:28:37:658 2011 H3C NQA/6/NQA_ENTRY_PROBE_RESULT: Reaction entry 1 of NQA entry admin-name 1 operation-tag 1: probe-pass.

*Jan 1 00:28:37:658 2011 H3C NQA/7/Reaction: NQA entry (1-1) reaction (1): Status changed from over-threshold to below-threshold.

*Jan 1 00:28:37:658 2011 H3C NQA/7/Reaction: NQA entry (1-1) reaction (1): Trigger notified.

*Jan 1 00:28:37:659 2011 H3C TRACK/7/Debug: Received the notification that the state of NQA (1-1) reaction (1) had changed to below-threshold.
*Jan 1 00:28:37:659 2011 H3C TRACK/7/Debug: The state of track entry 1 changed from Negative to Positive.
*Jan 1 00:28:37:660 2011 H3C TRACK/7/Debug: Track 1 status has changed, try to notify policy 2, eventkey 1, suppress time 0, last trigger time 1532.
%Jan 1 00:28:37:778 2011 H3C RTM/6/RTM_POLICY: CLI policy 2 is running successfully.
[H3C-GigabitEthernet0/4]dis cu
#
version 7.1.064, Release 0615P11
#
sysname H3C
#
dot1x
dot1x authentication-method eap
注意事项：
　　这种方法只能应对Radius服务器宕机的情况，如果服务器正常而Radius服务异常还是没有办法实现不装802.1X认证客户端免认证的需求