

某学校 S7506E portal认证报错

Portal 关萌 2018-09-26 发表

组网及说明

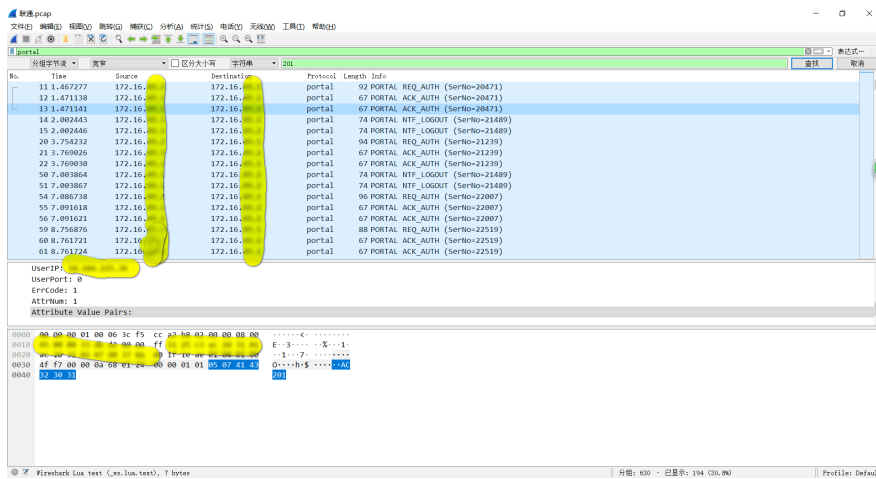
用户使用我司S7506E v7版本设备做为认证设备，使用第三方城市热点认证服务器做portal服务器同时为radius服务器。用户刚配置完后测试正常，在后续使用中出现问题大部分用户无法上线的情况。

问题描述

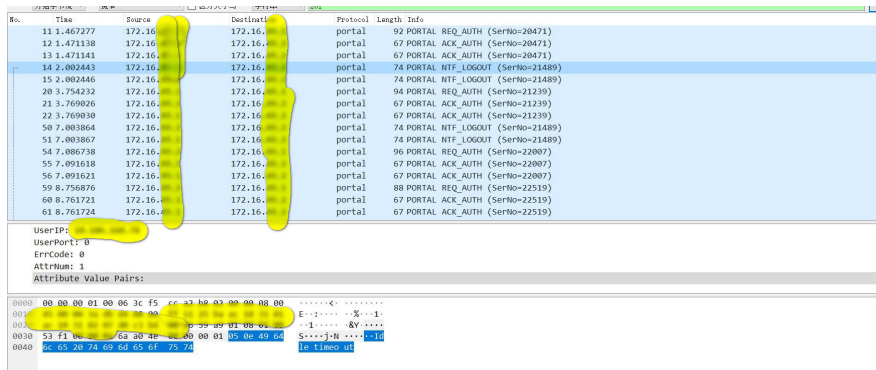
用户刚配置完后测试正常，在后续使用中出现问题大部分用户无法上线的情况。无法上线用户在终端上弹出portal页面后，输入用户名密码，点击登录按钮，会弹出认证失败报错。

用户反馈认证服务器收到设备回复的AC201错误，而后又收到NTF_LOGOUT报文，内容为Idle time out。

认证服务器收到的AC201错误报文如下



认证服务器收到Idle time out报错报文如下。



过程分析

通过对用户反馈的配置信息进行分析，发现设备配置正常。同时查询相关版本的已知问题，未发现Portal相关问题。通过收集debug信息进行进一步定位，通过收集debug信息发现，大量正常portal认证报文，但经过仔细排查发现有如下错误信息。设备调试信息中会有获取服务器信息失败的报错。于是设备对portal服务器回复了AC201信息。

*Sep 1 11:54:32:186 2018 BRAS RADIUS/7/EVENT: -MDC=1; Processing AAA request data.

*Sep 1 11:54:32:186 2018 BRAS RADIUS/7/EVENT: -MDC=1; Processing AAA request data.

*Sep 1 11:54:32:186 2018 BRAS RADIUS/7/EVENT: -MDC=1; Got request data successfully, primitive: authentication.

*Sep 1 11:54:32:186 2018 BRAS RADIUS/7/EVENT: -MDC=1; Getting RADIUS server info.

*Sep 1 11:54:32:187 2018 BRAS RADIUS/7/ERROR: -MDC=1; Failed to get server info.

*Sep 1 11:54:32:187 2018 BRAS RADIUS/7/EVENT: -MDC=1; Sent reply message successfully.

*Sep 1 11:54:32:187 2018 BRAS RADIUS/7/EVENT: -MDC=1;

Processing AAA request data.

*Sep 1 11:54:32:187 2018 BRAS RADIUS/7/EVENT: -MDC=1;

Processing AAA request data.

*Sep 1 11:54:32:187 2018 BRAS RADIUS/7/EVENT: -MDC=1;

Processing AAA request data.

*Sep 1 11:54:32:187 2018 BRAS RADIUS/7/EVENT: -MDC=1;

PAM_RADIUS: Processing RADIUS authentication.

*Sep 1 11:54:32:187 2018 BRAS RADIUS/7/EVENT: -MDC=1;

PAM_RADIUS: Fetched authentication reply-data successfully, resultCode: 3

*Sep 1 11:54:32:187 2018 BRAS PORTAL/7/FSM: -MDC=1; Auth-SM: Started to run.

*Sep 1 11:54:32:188 2018 BRAS PORTAL/7/PACKET: -MDC=1;

Portal sent 23 bytes of packet: Type=ack_auth(4), ErrCode=1, IP=10.107.64.21

*Sep 1 11:54:32:188 2018 BRAS PORTAL/7/PACKET: -MDC=1;

[5 TEXTINFO][7] [AC201]

通过调试信息，怀疑radius服务器状态异常，另用户反馈服务器状态信息，发现服务器状态正常为active状态。

<BRAS>dis radius scheme dr

RADIUS scheme name: dr

Index: 0

Primary authentication server:

IP : 172.16.*.* Port: 1812

VPN : Not configured

State: Active

Test profile: Not configured

Weight: 0

Primary accounting server:

IP : 172.16.*.* Port: 1813

VPN : Not configured

State: Active

Weight: 0

Accounting-On function : Enabled

extended function : Disabled

retransmission times : 50

retransmission interval(seconds) : 3

Timeout Interval(seconds) : 3

Retransmission Times : 3

Retransmission Times for Accounting Update : 5

Server Quiet Period(minutes) : 5

Realtime Accounting Interval(seconds) : 720

Stop-accounting packets buffering : Enabled

Retransmission times : 500

NAS IP Address : 172.16.*.*

Source IP Address : Not configured

VPN : Not configured

Username format : keep-original

Data flow unit : Byte

Packet unit : One

Attribute 15 check-mode : Strict

Attribute 25 : Standard

Remanent-Volume threshold : 0

Attribute Remanent-Volume unit : Kilo

Server-load-sharing : Disabled

Server-load-sharing mode : Session-based

Attribute 31 MAC format : HH-HH-HH-HH-HH-HH

Stop-accounting packets send-force : Disabled

RADIUS server version (vendor ID 2011) : 1.0

Authentication response pending limit : Not configured

Accounting response pending limit : Not configured

Username authorization : Not applied

通过以上信息看，可以确认当前服务器状态正常，怀疑服务器有可能有不稳定或性能不足情况，另用户反馈radius服务器统计信息和多次收集服务器状态，看是否有出现不正常情况，信息收集结果如下，服务器有很多重传、超时以及没有回复的报文统计，同时多次收集radius服务器状态也可以发现有服务

器被阻塞的情况。

<BRAS>dis radius statistics

	Auth.	Acct.	SessCtrl.	DAE.
Request Packet:	15032	15287	0	36
Retry Packet:	2616	46	-	0
Timeout Packet:	3923	68	-	-
Access Challenge:	0	-	-	-
Account Start:	-	714	-	-
Account Update:	-	13989	-	-
Account Stop:	-	584	-	-
Terminate Request:	-	-	0	36
Set Policy:	-	-	0	0
Packet With Response:	13725	15265	0	36
Packet Without Response:	1307	22	-	-
Access Rejects:	13008	-	-	-
Dropped Packet:	0	0	0	0
Check Failures:	0	0	0	0

<BRAS>dis radius scheme dr

RADIUS scheme name: dr

Index: 0

Primary authentication server:

IP : 172.16.*.* Port: 1812

VPN : Not configured

State: Block

Test profile: Not configured

Weight: 0

Primary accounting server:

IP : 172.16.*.* Port: 1813

VPN : Not configured

State: Active

Weight: 0

Accounting-On function : Enabled

extended function : Disabled

retransmission times : 50

retransmission interval(seconds) : 3

Timeout Interval(seconds) : 3

Retransmission Times : 3

Retransmission Times for Accounting Update : 5

Server Quiet Period(minutes) : 5

Realtime Accounting Interval(seconds) : 720

Stop-accounting packets buffering : Enabled

Retransmission times : 500

NAS IP Address : 172.16.*.*

Source IP Address : Not configured

VPN : Not configured

Username format : keep-original

Data flow unit : Byte

Packet unit : One

Attribute 15 check-mode : Strict

Attribute 25 : Standard

Remanent-Volume threshold : 0

Attribute Remanent-Volume unit : Kilo

Server-load-sharing : Disabled

Server-load-sharing mode : Session-based

Attribute 31 MAC format : HH-HH-HH-HH-HH-HH

Stop-accounting packets send-force : Disabled

RADIUS server version (vendor ID 2011) : 1.0

Authentication response pending limit : Not configured

Accounting response pending limit : Not configured

Username authorization : Not applied

当主服务器状态为active时，设备首先尝试与主服务器通信，若主服务器不可达，设备更改主服务器的状态为block，并启动该服务器的quiet定时器，然后按照从服务器的配置先后顺序依次查找状态为active的从服务器进行认证或者计费。如果状态为active的从服务器也不可达，则将该从服务器的状态置为b

lock, 同时启动该服务器的quiet定时器, 并继续查找状态为active的从服务器。当服务器的quiet定时器超时, 或者手动将服务器状态置为active时, 该服务器将恢复为active状态。在一次认证或计费过程中, 如果设备在尝试与从服务器通信时, 之前已经查找过的服务器状态由block恢复为active, 则设备并不会立即恢复与该服务器的通信, 而是继续查找从服务器。如果所有已配置的服务器都不可达, 则认为本次认证或计费失败。

通过以上信息可以看出, 为服务器软件、或服务器网上性能有限。大量用户同时上线, radius报文同时发向服务器过多, 导致服务器无法及时处理, 终端用户无法上线。

解决方法

调整优化服务器性能, 使用户认证报文得到及时处理, 同时按下表适当调大了服务器定时器时间。

表1 设置RADIUS服务器的定时器

操作	命令	说明
进入系统视图	system-view	-
进入RADIUS方案视图	radius scheme radius-scheme-name	-
设置RADIUS服务器响应超时时间	timer response-timeout seconds	缺省情况下, RADIUS服务器响应超时定时器为3秒
设置服务器恢复激活状态的时间	timer quiet minutes	缺省情况下, 服务器恢复激活状态前需要等待5分钟