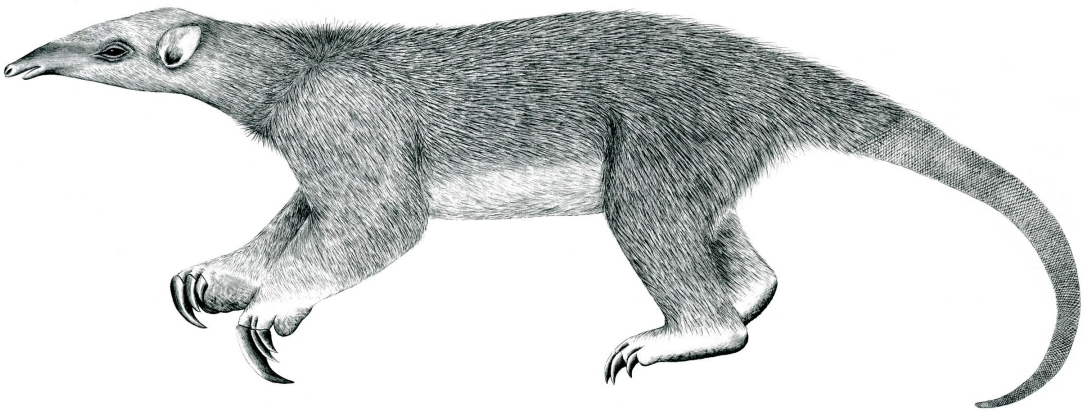
Tranalyzer2

radiusDecode

Remote Authentication Dial-In User Service (RADIUS)



Tranalyzer Development Team

Contents

1 radiusDecode

1.1 Description

The radiusDecode plugin analyzes RADIUS traffic.

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description
RADIUS_CNTS	1	Output counts, necessary for FORCE_MODE
RADIUS_AVPTYPE	1	Output AVP Types
RADIUS_NAS	1	Output NAS info
RADIUS_FRAMED	1	Output framed info
RADIUS_TUNNEL	1	Output tunnel info
RADIUS_ACCT	1	Output accounting info
RADIUS_NMS	0	Codes and AVP types format: 0: No code/type output 1: Values, 2: Names
RAD_CNTMX	20	Maximum number of codes/AVP types
RADIUS_STRMAX	128	Maximum length for strings

1.3 Flow File Output

The radiusDecode plugin outputs the following columns:

Column	Type	Description	Flags
radiusStat	H8	Status	
radiusAxsReq_Acc_Rej_Chal	4xU16	Access-Request/Accept/Reject/Challenge	RADIUS_CNTS=1
radiusAccReq_Resp	U16_U16	Accounting-Request/Response	RADIUS_CNTS=1
radiusAccStart_Stop	U16_U16	Accounting Start/Stop	RADIUS_CNTS=1
radiusCodes	R(U8)	Radius codes	RADIUS_NMS=1
radiusCodeNms	R(S)	Radius code names	RADIUS_NMS=2
radiusAVPTypes	R(U8)	AVP types	RADIUS_AVPTYPE=1&& RADIUS_NMS=1
radiusAVPTypeNms	R(S)	AVP type names	RADIUS_AVPTYPE=1&& RADIUS_NMS=2
radiusUser	S	Username	
radiusPW	S	Password	
radiusServiceType	U32	Service type	
radiusLoginService	U32	Login-Service	
radiusVendor	U32	Vendor Id (SMI)	

If RADIUS_NAS=1, the following columns are displayed:

Column	Type	Description	Flags
radiusNasId	S	NAS Identifier	
radiusNasIp	IP4	NAS IP address	
radiusNasPort	U32	NAS IP port	
radiusNasPortType	U32	NAS port type	
radiusNasPortId	S	NAS port Id	
If RADIUS_FRAMED=1, the following columns are displayed:			
radiusFramedIp	IP4	Framed IP address	
radiusFramedMask	IP4	Framed IP netmask	
radiusFramedProto	U32	Framed protocol	
radiusFramedComp	U32	Framed compression	
radiusFramedMtu	U32	Framed MTU	
If RADIUS_TUNNEL=1, the following columns are displayed:			
radiusTunnel_Medium	U32_U32	Tunnel type and medium type	
radiusTunnelCli	S	Tunnel client endpoint	
radiusTunnelSrv	S	Tunnel server endpoint	
radiusTunnelCliAId	S	Tunnel client authentication Id	
radiusTunnelSrvAId	S	Tunnel server authentication Id	
radiusTunnelPref	S	Tunnel preference	
If RADIUS_ACCT=1, the following columns are displayed:			
radiusAcctSessId	S	Accounting session Id	
radiusAcctSessTime	U32	Accounting session time (seconds)	
radiusAcctStatType	U32	Accounting status type	
radiusAcctTerm	U32	Accounting terminate cause	
radiusAcctInOct_OutOct	U32_U32	Accounting input/output octets	
radiusAcctInPkt_OutPkt	U32_U32	Accounting input/output packets	
radiusAcctInGw_OutGw	U32_U32	Accounting input/output gigawords	
radiusConnInfo	S	User connection info	
radiusFilterId	S	Filter Identifier	
radiusCalledId	S	Called Station Identifier	
radiusCallingId	S	Calling Station Identifier	
radiusReplyMsg	S	Reply message	

1.3.1 radiusStat

The radiusStat column is to be interpreted as follows:

radiusStat	Description
2^0 (=0x01)	Flow is RADIUS

radiusStat	Description
2^1 (=0x02)	Authentication and configuration traffic
2^2 (=0x04)	Accounting traffic
2^3 (=0x08)	—
2^4 (=0x10)	Connection successful
2^5 (=0x20)	Connection failed
2^6 (=0x40)	—
2^7 (=0x80)	Malformed packet

1.3.2 radiusServiceType

The `radiusServiceType` column is to be interpreted as follows:

radiusServiceType	Description
1	Login
2	Framed
3	Callback Login
4	Callback Framed
5	Outbound
6	Administrative
7	NAS Prompt
8	Authenticate Only
9	Callback NAS Prompt
10	Call Check
11	Callback Administrative
12	Voice
13	Fax
14	Modem Relay
15	IAPP-Register
16	IAPP-AP-Check
17	Authorize Only
18	Framed-Management
19	Additional-Authorization

1.3.3 radiusLoginService

The `radiusLoginService` column is to be interpreted as follows:

radiusLoginService	Description
0	Telnet
1	Rlogin
2	TCP Clear
3	PortMaster (proprietary)
4	LAT

radiusLoginService	Description
5	X25-PAD
6	X25-T3POS
7	Unassigned
8	TCP Clear Quiet (suppresses any NAS-generated connect string)

1.3.4 radiusVendor

The `radiusVendor` column represents the SMI Network Management Private Enterprise Codes which can be found at https://www.iana.org/assignments/enterprise-numbers. Alternatively use `grep` on the file `vendor.txt` as follows: `grep id vendor.txt`, where `id` is the actual Id reported by Tranalyzer, e.g., 4874 for Juniper.

1.3.5 radiusNasPortType

The `radiusNasPortType` column is to be interpreted as follows:

radiusNasPortType	Description
0	Async
1	Sync
2	ISDN Sync
3	ISDN Async V.120
4	ISDN Async V.110
5	Virtual
6	PIAFS
7	HDLC Clear Channel
8	X.25
9	X.75
10	G.3 Fax
11	SDSL - Symmetric DSL
12	ADSL-CAP - Asymmetric DSL, Carrierless Amplitude Phase Modulation
13	ADSL-DMT - Asymmetric DSL, Discrete Multi-Tone
14	IDSL - ISDN Digital Subscriber Line
15	Ethernet
16	xDSL - Digital Subscriber Line of unknown type
17	Cable
18	Wireless - Other
19	Wireless - IEEE 802.11
20	Token-Ring
21	FDDI
22	Wireless - CDMA2000
23	Wireless - UMTS
24	Wireless - 1X-EV
25	IAPP
26	FTTP - Fiber to the Premises
27	Wireless - IEEE 802.16
28	Wireless - IEEE 802.20

radiusNasPortType	Description
29	Wireless - IEEE 802.22
30	PPPoA - PPP over ATM
31	PPPoEoA - PPP over Ethernet over ATM
32	PPPoEoE - PPP over Ethernet over Ethernet
33	PPPoEoVLAN - PPP over Ethernet over VLAN
34	PPPoEoQinQ - PPP over Ethernet over IEEE 802.1QinQ
35	xPON - Passive Optical Network
36	Wireless - XGP
37	WiMAX Pre-Release 8 IWK Function
38	WIMAX-WIFI-IWK: WiMAX WIFI Interworking
39	WIMAX-SFF: Signaling Forwarding Function for LTE/3GPP2
40	WIMAX-HA-LMA: WiMAX HA and or LMA function
41	WIMAX-DHCP: WiMAX DCHP service
42	WIMAX-LBS: WiMAX location based service
43	WIMAX-WVS: WiMAX voice service

1.3.6 radiusFramedProto

The `radiusFramedProto` column is to be interpreted as follows:

radiusFramedProto	Description
1	PPP
2	SLIP
3	AppleTalk Remote Access Protocol (ARAP)
4	Gandalf proprietary SingleLink/MultiLink protocol
5	Xylogics proprietary IPX/SLIP
6	X.75 Synchronous
7	GPRS PDP Context

1.3.7 radiusFramedComp

The `radiusFramedComp` column is to be interpreted as follows:

radiusFramedComp	Description
0	None
1	VJ TCP/IP header compression
2	IPX header compression
3	Stac-LZS compression

1.3.8 radiusTunnel_Medium

The `radiusTunnel_Medium` column is to be interpreted as follows:

radiusTunnel	Description
1	Point-to-Point Tunneling Protocol (PPTP)
2	Layer Two Forwarding (L2F)
3	Layer Two Tunneling Protocol (L2TP)
4	Ascend Tunnel Management Protocol (ATMP)
5	Virtual Tunneling Protocol (VTP)
6	IP Authentication Header in the Tunnel-mode (AH)
7	IP-in-IP Encapsulation (IP-IP)
8	Minimal IP-in-IP Encapsulation (MIN-IP-IP)
9	IP Encapsulating Security Payload in the Tunnel-mode (ESP)
10	Generic Route Encapsulation (GRE)
11	Bay Dial Virtual Services (DVS)
12	IP-in-IP Tunneling
13	Virtual LANs (VLAN)

radiusMedium	Description
1	IPv4 (IP version 4)
2	IPv6 (IP version 6)
3	NSAP
4	HDLC (8-bit multidrop)
5	BBN 1822
6	802 (includes all 802 media plus Ethernet “canonical format”)
7	E.163 (POTS)
8	E.164 (SMDS, Frame Relay, ATM)
9	F.69 (Telex)
10	X.121 (X.25, Frame Relay)
11	IPX
12	Appletalk
13	Decnet IV
14	Banyan Vines
15	E.164 with NSAP format subaddress

1.3.9 radiusAcctStatType

The `radiusAcctStatType` column is to be interpreted as follows:

radiusAcctStatType	Description
1	Start
2	Stop
3	Interim-Update
7	Accounting-On
8	Accounting-Off
9	Tunnel-Start
10	Tunnel-Stop

radiusAcctStatType	Description
11	Tunnel-Reject
12	Tunnel-Link-Start
13	Tunnel-Link-Stop
14	Tunnel-Link-Reject
15	Failed

1.3.10 radiusAcctTerm

The `radiusAcctTerm` column is to be interpreted as follows:

radiusAcctTerm	Description
1	User Request
2	Lost Carrier
3	Lost Service
4	Idle Timeout
5	Session Timeout
6	Admin Reset
7	Admin Reboot
8	Port Error
9	NAS Error
10	NAS Request
11	NAS Reboot
12	Port Unneeded
13	Port Preempted
14	Port Suspended
15	Service Unavailable
16	Callback
17	User Error
18	Host Request
19	Supplicant Restart
20	Reauthentication Failure
21	Port Reinitialized
22	Port Administratively Disabled
23	Lost Power

1.4 Packet File Output

In packet mode (`-s` option), the radiusDecode plugin outputs the following columns:

Column	Type	Description	Flags
radiusStat	H8	Status	
radiusCode	U8	Code	RADIUS_NMS=1
radiusCodeNm	S	Code name	RADIUS_NMS=2
radiusAVPTypes	R(U8)	AVP types	RADIUS_AVPTYPE=1&&RADIUS_NMS=1

Column	Type	Description	Flags
radiusAVPTypeNms	R(S)	AVP type names	RADIUS_AVPTYPE=1&&RADIUS_NMS=2

1.5 Monitoring Output

In monitoring mode, the radiusDecode plugin outputs the following columns:

Column	Type	Description	Flags
radiusPkts	U64	Number of RADIUS packets	
radiusAxsPkts	U64	Number of Access	
radiusAxsAccPkts	U64	Number of Access-Accept	
radiusAxsRejPkts	U64	Number of Access-Reject	
radiusAccPkts	U64	Number of Accounting packets	

1.6 Plugin Report Output

The following information is reported:

- Aggregated radiusStat
- Number of RADIUS packets
- Number of Access, Access-Accept, Access-Reject and Accounting packets

1.7 References

- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868: RADIUS Attributes for Tunnel Protocol Support
- RFC2869: RADIUS Extensions
- https://www.iana.org/assignments/radius-types/radius-types.xhtml