RSA NetWitness Platform

Event Source Log Configuration Guide

RSA NetFlow Collector

Last Modified: Tuesday, April 6, 2021

Event Source Product Information:

Vendor: RSA, The Security Division of EMC
Event Source: NetFlow Collection Module
Versions: 10.4

RSA Product Information:

Supported On: Security Analytics 10.4 and later
Event Source Log Parser: rsaflow, cef
Collection Method: Netflow
Event Source Class.Subclass: Security.Analysis

Configure RSA NetFlow Collection Module

To configure NetFlow collection for an event source, you must perform the following procedures:

- Configure RSA NetWitness Platform for NetFlow Collection. Search for **Configure NetFlow Event Sources** in the RSA NetWitness Platform help.
- Configure NetFlow Output on the event source. See the associated documentation for each individual event source for help in configuring the event source to send NetFlow data.

About NetFlow

NetFlow was created for the purpose of generating flow information, (source IP, source port, destination IP, destination port). That flow information is then used for optimizing network flow through the routers and switches. Additionally, the flow information generated is useful for reporting and providing useful insights from a RSA NetWitness Platform perspective.

NetFlow reports the flow information by way of flow records. These records contain the packet/byte count of a unidirectional flows. The netflow records are assembled into export datagrams, with up to 30 records per datagram. A NetFlow collector collects these datagrams.

The RSA NetFlow collection module can parse both Version 5 and Version netflow export datagrams.

NetFlow Collector Mapping

The collector file, `netflow.xml`, is responsible for mapping NetFlow v5 and v9 flow record fields. The fields are mapped according to these rules:

1. If the NetFlow field has an equivalent in the Common Event Format (CEF) standard, then the field is mapped to the CEF field.
2. If the NetFlow v5 field has an equivalent v9 field, then the v5 field is mapped to the v9 field.
3. Otherwise, the original NetFlow field remains unchanged.

NetFlow Collector Mapping File

Separate sections exist for v5 and v9 and these are further separated into **Header** and **Data** sections.

Note the following:

- The **<in>** value is how the field appears in the log message before mapping is applied.
- The **<out>** value is the field name that is sent to the RSA Log Decoder.
- To enable a field to be included in the log message, set **<inc>** to true.

- To disable a field, set **<inc>** to false.
- The field **<fmt>** determines the output format of the field.

NetFlow Mapping File Details

The following tables describe the fields available, and their mappings as they are parsed through RSA NetWitness Platform.

Note that the **Index** field is listed in all of the following tables, so that you can compare the row details across the presented tables.

NetFlow Details

This tables describes the NetFlow information.

Index	v9 Field	v5 Field	Description	Format
0	Invalid	Invalid	Unrecognized key	DEC
1	InBytes	[none]	Incoming counter for number of bytes associated with an IP Flow.	DEC
2	InPackets	[none]	Incoming counter for the number of packets associated with an IP Flow	DEC
3	Flows	SequenceCounter	Number of flows that were aggregated. SequenceCounter in NetFlow Version 5 and Version 8 headers represented “total flows.”	DEC
4	Protocol	IpProtocol	IP protocol	DEC

Index	v9 Field	v5 Field	Description	Format
5	SrcTos	TypeOfService	Type of Service setting when entering incoming interface	DEC
6	TcpFlags	TcpFlags	Cumulative of all the TCP flags seen for this flow	DEC
7	L4SrcPort	SrcPort	TCP/UDP source port number. For example, FTP, Telnet, or equivalent	DEC
8	Ipv4SrcAddr	SrcAddr	IPv4 source address	IP
9	SrcMask	SrcPrefixMask	Source address subnet mask, in slash notation	PREFIX
10	InputSnmp	SNMPinputIF	Input interface index	DEC
11	L4DstPort	DstPort	TCP/UDP destination port number, e.g. FTP, Telnet, or equivalent	DEC
12	Ipv4DstAddr	DstAddr	IPv4 destination address	IP
13	DstMask	DstPrefixMask	The number of contiguous bits in the source address subnet, in slash notation	PREFIX
14	OutputSnmp	SNMPoutputIF	Output interface index	DEC

Index	v9 Field	v5 Field	Description	Format
15	Ipv4NextHop	NextHopAddr	IPv4 address of next-hop router	IP
16	SrcAs	SrcAutoSysNum	Source BGP autonomous system number	DEC
17	DstAs	DstAutoSysNum	Destination BGP autonomous system number	DEC
18	BgpIpv4NextHop	[none]	Next-hop router's IP in the BGP domain	DEC
19	MulDstPkts	[none]	IP multicast outgoing packet counter	DEC
20	MulDstBytes	[none]	IP multicast outgoing byte counter	DEC
21	FirstSwitched	StartUpTime	System uptime at which the first packet of this flow was switched	DEC
22	LastSwitched	LastUptime	System uptime at which the last packet of this flow was switched	DEC
23	OutBytes	[none]	Outgoing counter for the number of bytes associated with an IP Flow	DEC

Index	v9 Field	v5 Field	Description	Format
24	OutPackets	[none]	Outgoing counter for the number of packets associated with an IP Flow.	DEC
25	MinPacketLen	[none]	Minimum IP packet length on incoming packets of the flow	DEC
26	MaxPacketLen	[none]	Maximum IP packet length on incoming packets of the flow	DEC
27	Ipv6SrcAddr	[none]	IPv6 Source Address	IP
28	Ipv6DstAddr	[none]	IPv6 Destination Address	IP
29	Ipv6SrcMask	[none]	IPv6 source mask	DEC
30	Ipv6DstMask	[none]	IPv6 destination mask	DEC
31	Ipv6FlowLabel	[none]	IPv6 flow label as per RFC 2460 definition	HEX
32	IcmpType	[none]	Internet Control Message Protocol (ICMP) packet type; reported as ((ICMP Type*256) + ICMP code)	DEC
33	MulIgmpType	[none]	Internet Group Management Protocol (IGMP) packet type	DEC

Index	v9 Field	v5 Field	Description	Format
34	SamplingInterval	Sampling	When using sampled NetFlow, the rate at which packets are sampled i.e.: a value of 100 indicates that one of every 100 packets is sampled	DEC
35	SamplingAlgorithm	[none]	The type of algorithm used for sampled: • NetFlow: 0x01 • Deterministic Sampling:0x02 • Random Sampling: 0x03	DEC
36	FlowActiveTimeout	[none]	Timeout value (in seconds) for active flow entries in the NetFlow cache	DEC
37	FlowInactiveTimeout	[none]	Timeout value (in seconds) for inactive flow entries in the NetFlow cache	DEC
38	EngineType	EngineType	Type of flow switching engine: RP = 0, VIP/Linecard = 1	DEC
39	EngineId	EngineId	ID number of the flow switching engine	DEC
40	TotalBytesExp	[none]	Counter for the num-	DEC

Index	v9 Field	v5 Field	Description	Format
			ber of bytes exported by the Observation Domain	
41	TotalPacketsExp	[none]	Counter for bytes for the number of packets exported by the Observation Domain	DEC
42	TotalFlowsExp	[none]	Counter for the number of flows exported by the Observation Domain	DEC
43	VendorSpecific1	[none]	Vendor defined field	DEC
44	Ipv4SrcPrefix	[none]	IPv4 source address prefix (specific for Catalyst architecture)	IP
45	Ipv4DstPrefix	[none]	"IPv4 destination address prefix (specific for Catalyst architecture)"	
46	MplsTopLabelType	[none]	MPLS Top Label Type	DEC
47	MplsTopLabelIpAddr	[none]	Forwarding Equivalent Class corresponding to the MPLS Top Label	DEC
48	FlowSamplerId	[none]	Identifier shown in “show flow-sampler”	DEC

Index	v9 Field	v5 Field	Description	Format
49	FlowSamplerMode	[none]	The type of algorithm used for sampling data. Use in connection with SamplingAlgorithm	DEC
50	FlowSamplerRandIntv	[none]	Packet interval at which to sample. Use in connection with FlowSamplerMode	DEC
51	VendorSpecific2	[none]	Vendor defined field	STR
52	MinTtl	[none]	Minimum TTL on incoming packets of the flow	DEC
53	MaxTtl	[none]	Maximum TTL on incoming packets of the flow	DEC
54	Ipv4Ident	[none]	The IP v4 identification field	DEC
55	DstTos	[none]	Type of Service byte setting when exiting outgoing interface	DEC
56	InSrcMac	[none]	Incoming source MAC address	MAC
57	OutDstMac	[none]	Outgoing destination MAC address	MAC

Index	v9 Field	v5 Field	Description	Format
58	SrcVlan	[none]	Virtual LAN identifier associated with ingress interface	DEC
59	DstVlan	[none]	Virtual LAN identifier associated with egress interface	DEC
60	IpProtoVersion	[none]	Internet Protocol Version Set to 4 for IPv4, set to 6 for IPv6. If not present in the template, then version 4 is assumed.	DEC
61	Direction	[none]	Flow direction: 0 - ingress flow, 1 - egress flow	DEC
62	Ipv6NextHop	[none]	IPv6 address of the next-hop router	IP
63	BgpIpv6NextHop	[none]	Next-hop router in the BGP domain	IP
64	Ipv6OptionHeaders	[none]	Identifies IPv6 option headers found in the flow	HEX
65	VendorSpecific3	[none]	Vendor defined field	DEC
66	VendorSpecific4	[none]	Vendor defined field	DEC
67	VendorSpecific5	[none]	Vendor defined field	DEC

Index	v9 Field	v5 Field	Description	Format
68	VendorSpecific6	[none]	Vendor defined field	DEC
69	VendorSpecific7	[none]	Vendor defined field	DEC
70	MplsLabel1	[none]	MPLS label at position 1 in the stack.	DEC
71	MplsLabel2	[none]	MPLS label at position 2 in the stack.	DEC
72	MplsLabel3	[none]	MPLS label at position 3 in the stack.	DEC
73	MplsLabel4	[none]	MPLS label at position 4 in the stack.	DEC
74	MplsLabel5	[none]	MPLS label at position 5 in the stack.	DEC
75	MplsLabel6	[none]	MPLS label at position 6 in the stack.	DEC
76	MplsLabel7	[none]	MPLS label at position 7 in the stack.	DEC
77	MplsLabel8	[none]	MPLS label at position 8 in the stack.	DEC
78	MplsLabel9	[none]	MPLS label at position 9 in the stack.	DEC
79	MplsLabel10	[none]	MPLS label at position 10 in the stack.	DEC
80	InDstMac	[none]	Incoming destination MAC address	MAC

Index	v9 Field	v5 Field	Description	Format
81	OutSrcMac	[none]	Outgoing source MAC address	MAC
82	IfName	[none]	Shortened interface name i.e.: “FE1/0”	STR
83	IfDesc	[none]	Full interface name i.e.: “'FastEthernet 1/0”	STR
84	SamplerName	[none]	Name of the flow sampler	STR
85	InPermBytes	[none]	Running byte counter for a permanent flow	DEC
86	InPermPackets	[none]	Running packet counter for a per-manent flow	DEC
87	VendorSpecific8	[none]	Vendor defined field	DEC
[none]	[none]	UnixNSeconds	Residual nanoseconds since 0000 UTC 1970	DEC
[none]	[none]	OctetsInFlow	Total number of Layer 3 bytes in the packets of the flow	DEC
[none]	[none]	PacketsInFlow	Packets in the flow	DEC

Index	v9 Field	v5 Field	Description	Format
header	SequenceCounter	[none]	Incremental sequence counter of all export packets sent by this export device; this value is cumulative, and it can be used to identify whether any export packets have been missed. Note: This is a change from the NetFlow Version 5 and Version 8 headers, where this number represented “total flows.”	DEC
header	sourceId	[none]	The Source ID field is used to guarantee uniqueness for all flows exported from a particular device. (The Source ID field is the equivalent of the engine type and engine ID fields found in the NetFlow Version 5 and Version 8 headers). The format of this field is vendor specific.	DEC

Index	v9 Field	v5 Field	Description	Format
header	SystemUpTime	SystemUpTime	Time in milliseconds since this device was first booted	DEC
header	templateId	[none]	As a router generates different template FlowSets to match the type of NetFlow data it will be exporting, each template is given a unique ID. This uniqueness is local to the router that generated the template ID. Templates that define data record formats begin numbering at 256 since 0-255 are reserved for FlowSet IDs.	DEC
header	UnixSeconds	UnixSeconds	Seconds since 0000 Coordinated Universal Time (UTC) 1970	DEC
header	Version	Version	The version of NetFlow records exported in this packet; for Version 9, this value is 0x0009	DEC

CEF Details

This tables lists the CEF information.

Index	Key	Full Name	Key Format	Description
0	[none]	[none]	[none]	[none]
1	in	bytesIn	Integer	Number of bytes transferred inbound. Inbound relative to the source to destination relationship, meaning that data was flowing from source to destination.
2	[none]	[none]	[none]	[none]
3	cnt	baseEventCount	Integer	A count associated with this event.
4	proto	transport Protocol	string	Identifies the Layer-4 protocol used. The possible values are protocol names such as TCP or UDP.

Index	Key	Full Name	Key Format	Description
5	[none]	[none]	[none]	[none]
6	[none]	[none]	[none]	[none]
7	spt	sourcePort	integer	The valid port numbers are 0 to 65535.
8	src	SourceAddress	IPv4Address	Identifies the source that an event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”
9	[none]	[none]	[none]	[none]
10	[none]	[none]	[none]	[none]
11	dpt	destinationPort	integer	The valid port numbers are between 0 and 65535.
12	dst	destinationAddress	IPv4Address	Identifies destination that the event refers to in an IP network. The format is an IPv4 address.

Index	Key	Full Name	Key Format	Description
				Example: “192.168.10.1”
13	[none]	[none]	[none]	[none]
14	[none]	[none]	[none]	[none]
15	[none]	[none]	[none]	[none]
16	[none]	[none]	[none]	[none]
17	[none]	[none]	[none]	[none]
18	[none]	[none]	[none]	[none]
19	[none]	[none]	[none]	[none]
20	[none]	[none]	[none]	[none]
21	[none]	startTime	Timestamp	The time when the activity the event referred to started. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st 1970).
22	[none]	endTime	Timestamp	The time at which the activity related to the event ended. The

Index	Key	Full Name	Key Format	Description
				format is MMM dd yyyy HH:m-m:ss or mil-liseconds since epoch (Jan 1st 1970). An example would be reporting the end of a session.
23	out	bytesOut	integer	Number of bytes transferred out-bound. Outbound relative to the source to des-tination rela-tionship, meaning that data was flowing from des-tination to source.
24	[none]	[none]	[none]	[none]
25	[none]	[none]	[none]	[none]
26	[none]	[none]	[none]	[none]
27	[none]	[none]	[none]	[none]
28	[none]	[none]	[none]	[none]
29	[none]	[none]	[none]	[none]

Index	Key	Full Name	Key Format	Description
30	[none]	[none]	[none]	[none]
31	[none]	[none]	[none]	[none]
32	[none]	[none]	[none]	[none]
33	[none]	[none]	[none]	[none]
34	[none]	[none]	[none]	[none]
35	[none]	[none]	[none]	[none]
36	[none]	[none]	[none]	[none]
37	[none]	[none]	[none]	[none]
38	[none]	[none]	[none]	[none]
39	[none]	[none]	[none]	[none]
40	[none]	[none]	[none]	[none]
41	[none]	[none]	[none]	[none]
42	[none]	[none]	[none]	[none]
43	cs1	deviceCustomString1	string	There are six strings available which can be used to map fields which do not fit into any other field of this dictionary.
44	[none]	[none]	[none]	[none]

Index	Key	Full Name	Key Format	Description
45	[none]	[none]	[none]	[none]
46	[none]	[none]	[none]	[none]
47	[none]	[none]	[none]	[none]
48	[none]	[none]	[none]	[none]
49	[none]	[none]	[none]	[none]
50	[none]	[none]	[none]	[none]
51	cs2	deviceCustomString2	string	There are six strings available which can be used to map fields which do not fit into any other field of this dictionary.
52	[none]	[none]	[none]	[none]
53	[none]	[none]	[none]	[none]
54	[none]	[none]	[none]	[none]
55	[none]	[none]	[none]	[none]
56	smac	sourceMacAddress	MAC address	Six colon-separated hexadecimal numbers.

Index	Key	Full Name	Key Format	Description
57	dmac	destinationMac Address	MAC address	Six colon-separated hexadecimal numbers.
58	[none]	[none]	[none]	[none]
59	[none]	[none]	[none]	[none]
60	[none]	[none]	[none]	[none]
61	deviceDirection	deviceDirection	String	Any information about what direction the communication that was observed has taken.
62	[none]	[none]	[none]	[none]
63	[none]	[none]	[none]	[none]
64	[none]	[none]	[none]	[none]
65	cs3	deviceCustomString3	String	There are six strings available which can be used to map fields which do not fit into any other field of this dictionary.

Index	Key	Full Name	Key Format	Description
66	cs4	deviceCustomString4	String	There are six strings available which can be used to map fields which do not fit into any other field of this dictionary.
67	cs5	deviceCustomString5	String	There are six strings available which can be used to map fields which do not fit into any other field of this dictionary.
68	cs6	deviceCustomString6	String	There are six strings available which can be used to map fields which do not fit into any other field of this dictionary.
69	[none]	[none]	[none]	[none]
70	[none]	[none]	[none]	[none]

Index	Key	Full Name	Key Format	Description
71	[none]	[none]	[none]	[none]
72	[none]	[none]	[none]	[none]
73	[none]	[none]	[none]	[none]
74	[none]	[none]	[none]	[none]
75	[none]	[none]	[none]	[none]
76	[none]	[none]	[none]	[none]
77	[none]	[none]	[none]	[none]
78	[none]	[none]	[none]	[none]
79	[none]	[none]	[none]	[none]
80	dmac	destinationMac Address	MAC address	Six colon-separated hexadecimal numbers.
81	smac	sourceMacAddress	MAC address	Six colon-separated hexadecimal numbers.
82	[none]	deviceInboundInterface / deviceOutboundInterface	String	Interface on which the packet or data entered / left the device.
83	[none]	[none]	[none]	[none]

Index	Key	Full Name	Key Format	Description
84	[none]	[none]	[none]	[none]
85	[none]	[none]	[none]	[none]
86	[none]	[none]	[none]	[none]
87	[none]	[none]	[none]	[none]
[none]	[none]	[none]	[none]	[none]
[none]	[none]	[none]	[none]	[none]
[none]	[none]	[none]	[none]	[none]
header	[none]	[none]	[none]	[none]
header	externalId	externalId	Integer	An ID used by the originating device. Usually these are increasing numbers associated with events
header	[none]	[none]	[none]	[none]
header	[none]	[none]	[none]	[none]

Index	Key	Full Name	Key Format	Description
header	rt	receiptTime	Timestamp	The time at which the event related to the activity was received. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st 1970).
header	[none]	[none]	[none]	[none]

RSA Details

This table describes the RSA parsing information.

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsaflowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
0	Invalid	cn_invalid	[none]	[none]	[none]
1	in	rbytes	[none]	rbytes	Bytes received
2	InPackets	cn_rpackets	[none]	[none]	n/a

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsaflowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
3	cnt	event_counter	[none]	event.-counter	Number of times the event has repeated, OR The Total number of events aggregated.
4	proto	ip_proto	ip.proto	protocol	IP protocol name
5	SrcTos	cn_src_tos	[none]	tos	The priority given to a network protocol
6	TcpFlags	tcp_flags	tcp.flags	[none]	(TCP only) bit-packed denoting which flags were seen in the session, regardless of client or server and

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsa-flowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
					regardless of how many times that flag was seen.
7	spt	sport	tcp.srcport / udp.srcport	ip.srcport	Source port
8	src	saddr	ip.src	ip.src	Source IPv4 address
9	SrcMask	smask	[none]	smask	Source device network mask
10	InputSnmp	dinterface	[none]	sinterface	Network Source interface
11	dpt	dport	tcp.dstport / udp.dstport	ip.dstport	Destination port
12	dst	daddr	ip.dst	ip.dst	Destination address

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsaflowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
13	DstMask	dmask	[none]	dmask	Destination Device network mask
14	OutputSnmp	sinterface	[none]	sinterface	Network Source interface
15	Ipv4NextHop	cs_ip_next_hop	[none]	[none]	[none]
16	SrcAs	cn_asn_src	asn.src	[none]	Source BGP autonomous system number
17	DstAs	cn_asn_dst	asn.dst	[none]	Destination BGP autonomous system number
18	BgpIpv4NextHop	cn_bgp_ipv4_next_hop	[none]	[none]	[none]
19	MulDstPkts	cn_mul_dst_pks	[none]	[none]	[none]
20	MulDstBytes	cn_mul_dst_	[none]	[none]	[none]

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsa-flowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
		bytes			
21	FirstSwitched	cn_first_switched	[none]	[none]	Start time of the event. If you are using this you MUST also be using **event_time**.
22	LastSwitched	cn_last_switched	[none]	[none]	[none]
23	out	sbytes	[none]	bytes	Bytes sent
24	OutPackets	cn_spackets	[none]	packets	n/a
25	MinPacketLen	cn_min_packet_len	[none]	[none]	[none]
26	MaxPacketLen	cn_max_packet_len	[none]	[none]	[none]
27	src	saddr	ipv6.src	ipv6.src	Source IPv6 Address

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsaflowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
28	dst	daddr	ipv6.dst	ipv6.dst	Destination IPv6 Address
29	Ipv6SrcMask	smask	[none]	smask	Source device network mask
30	Ipv6DstMask	dmask	[none]	dmask	Destination device network mask
31	Ipv6FlowLabel	cn_ipv6_flow_label	[none]	[none]	[none]
32	IcmpType	icmptype	[none]	icmp.type / icmp.code	The "type" value for an ICMP packet. / The "code" value for an ICMP packet.
33	MulIgmpType	cn_mul_igmp_type	[none]	[none]	[none]
34	SamplingInterval	cn_sampling_	[none]	[none]	[none]

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsaflowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
		interval			
35	SamplingAlgorithm	cn_sampling_algorithm	[none]	[none]	[none]
36	FlowActiveTimeout	cn_flow_active_timeout	[none]	[none]	[none]
37	FlowInactiveTimeout	cn_flow_inactive_timeout	[none]	[none]	[none]
38	EngineType	cn_engine_type	[none]	[none]	[none]
39	EngineId	cn_engine_id	[none]	[none]	[none]
40	TotalBytesExp	cn_total_bytes_exp	[none]	[none]	[none]
41	TotalPacketsExp	cn_total_packets_exp	[none]	[none]	[none]
42	TotalFlowsExp	cn_total_flows_exp	[none]	[none]	[none]
43	cs1	fld	[none]	[none]	[none]
44	Ipv4SrcPrefix	cs_ipv4_src_prefix	[none]	[none]	[none]

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsaflowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
45	Ipv4DstPrefix	cs_ipv4_dst_prefix	[none]	[none]	[none]
46	MplsTopLabelType	cn_mpls_top_label_type	[none]	[none]	[none]
47	MplsTopLabelIpAddr	cn_mpls_top_label_ipaddr	[none]	[none]	[none]
48	FlowSamplerId	cn_flow_sampler_id	[none]	[none]	[none]
49	FlowSamplerMode	cn_flow_sampler_mode	[none]	[none]	[none]
50	FlowSamplerRandIntv	cn_flow_sampler_rand_intv	[none]	[none]	[none]
51	cs2	fld	[none]	[none]	[none]
52	MinTtl	cn_min_ttl	[none]	[none]	[none]
53	MaxTtl	cn_max_ttl	[none]	[none]	[none]
54	Ipv4Ident	cn_ipv4_ident	[none]	[none]	[none]

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsa-flowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
55	DstTos	cn_dst_tos	[none]	tos	The priority given to a network protocol
56	smac	smacaddr	eth.src	eth.src	Source MAC address
57	dmac	dmacaddr	eth.dst	eth.dst	Destination MAC address
58	SrcVlan	cn_src_vlan	[none]	vlan.name	VLAN number
59	DstVlan	cn_dst_vlan	[none]	vlan.name	VLAN number
60	IpProtoVersion	cn_ip_proto_version	[none]	[none]	[none]

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsaflowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
61	deviceDirection	direction	[none]	direction	Direction of the network flow (for the systems that capture this)
62	Ipv6NextHop	cs_ipv6_next_hop	[none]	[none]	[none]
63	BgpIpv6NextHop	cs_bgp_ipv6_next_hop	[none]	[none]	[none]
64	Ipv6OptionHeaders	cn_ipv6_option_headers	[none]	[none]	[none]
65	cs3	fld	[none]	[none]	[none]
66	cs4	fld	[none]	[none]	[none]
67	cs5	fld	[none]	[none]	[none]
68	cs6	fld	[none]	[none]	[none]
69	cs7	fld	[none]	[none]	[none]
70	MplsLabel1	cn_mpls_label_1	[none]	[none]	[none]

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsa-flowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
71	MplsLabel2	cn_mpls_label_2	[none]	[none]	[none]
72	MplsLabel3	cn_mpls_label_3	[none]	[none]	[none]
73	MplsLabel4	cn_mpls_label_4	[none]	[none]	[none]
74	MplsLabel5	cn_mpls_label_5	[none]	[none]	[none]
75	MplsLabel6	cn_mpls_label_6	[none]	[none]	[none]
76	MplsLabel7	cn_mpls_label_7	[none]	[none]	[none]
77	MplsLabel8	cn_mpls_label_8	[none]	[none]	[none]
78	MplsLabel9	cn_mpls_label_9	[none]	[none]	[none]
79	MplsLabel10	cn_mpls_label_10	[none]	[none]	[none]
80	dmac	dmacaddr	eth.dst	eth.dst	Destination MAC address
81	smac	smacaddr	eth.src	eth.src	Source MAC address
82	IfName	cs_if_name	[none]	[none]	[none]
83	IfDesc	cs_if_desc	[none]	[none]	[none]

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsaflowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
84	SamplerName	cs_sampler_name	[none]	[none]	[none]
85	InPermBytes	cn_in_perm_bytes	[none]	[none]	[none]
86	InPermPackets	cn_in_perm_packets	[none]	[none]	[none]
87	cs8	fld	[none]	[none]	[none]
[none]	UnixNSeconds	cn_unix_nano_seconds	[none]	[none]	[none]
[none]	OctetsInFlow	bytes	size	bytes	Total bytes
[none]	PacketsInFlow	packets	packets	packets	Total packets
header	SequenceCounter	cn_sequence_counter	[none]	[none]	[none]
header	externalId	hardware_id	[none]	hardware.id	A unique identifier for a device or system (NOT a Mac

Index	Flow Collector Mapping (netflow.xml)	Flow Parser Mapping (rsaflowmsg.xml)	NetWitness Platform Network Meta Key	NetWitness Platform Log Mapping Meta Key	Description
					address)
header	SystemUpTime	cn_system_uptime_ms	[none]	[none]	[none]
header	TemplateId	cn_template_id	[none]	[none]	[none]
header	rt	event_time	[none]	event.time	Date/Time of the occurrence of the event as recorded by the system which generated it.
header	Version	version	[none]	version	Version of the application or OS which is generating the event.

Table Map Details

This table contains details for the Table-Map.xml file.

Index	enVision Name	NetWitness Platform Name	Failure Key
0	[none]	n/a	n/a
1	rbytes	rbytes	n/a
2	[none]	n/a	n/a
3	event_counter	event.counter	n/a
4	ip_proto	ip.proto	protocol
5	tos	tos	n/a
6	tcp_flags	tcp.flags	n/a
7	sport	ip.srcport	n/a
8	saddr	ip.src	ipv6.src
9	smask	smask	n/a
10	sinterface	sinterface	n/a
11	dport	ip.dstport	n/a
12	daddr	ip.dst	ipv6.dst
13	dmask	dmask	n/a
14	sinterface	sinterface	n/a
15	[none]	n/a	n/a

Index	enVision Name	NetWitness Platform Name	Failure Key
16	[none]	n/a	n/a
17	[none]	n/a	n/a
18	[none]	n/a	n/a
19	[none]	n/a	n/a
20	[none]	n/a	n/a
21	[none]	n/a	n/a
22	[none]	n/a	n/a
23	sbytes	bytes.src	n/a
24	[none]	n/a	n/a
25	[none]	n/a	n/a
26	[none]	n/a	n/a
27	saddr_v6	ipv6.src	n/a
28	daddr_v6	ipv6.dst	n/a
29	smask	smask	n/a
30	dmask	dmask	n/a
31	[none]	n/a	n/a
32	icmptype	icmp.type	n/a
33	[none]	n/a	n/a
34	[none]	n/a	n/a

Index	enVision Name	NetWitness Platform Name	Failure Key
35	[none]	n/a	n/a
36	[none]	n/a	n/a
37	[none]	n/a	n/a
38	[none]	n/a	n/a
39	[none]	n/a	n/a
40	[none]	n/a	n/a
41	[none]	n/a	n/a
42	[none]	n/a	n/a
43	[none]	n/a	n/a
44	[none]	n/a	n/a
45	[none]	n/a	n/a
46	[none]	n/a	n/a
47	[none]	n/a	n/a
48	[none]	n/a	n/a
49	[none]	n/a	n/a
50	[none]	n/a	n/a
51	[none]	n/a	n/a
52	[none]	n/a	n/a
53	[none]	n/a	n/a

Index	enVision Name	NetWitness Platform Name	Failure Key
54	[none]	n/a	n/a
55	tos	tos	n/a
56	smacaddr	eth.src	n/a
57	dmacaddr	eth.dst	n/a
58	[none]	n/a	n/a
59	[none]	n/a	n/a
60	[none]	n/a	n/a
61	direction	direction	n/a
62	[none]	n/a	n/a
63	[none]	n/a	n/a
64	[none]	n/a	n/a
65	[none]	n/a	n/a
66	[none]	n/a	n/a
67	[none]	n/a	n/a
68	[none]	n/a	n/a
69	[none]	n/a	n/a
70	[none]	n/a	n/a
71	[none]	n/a	n/a
72	[none]	n/a	n/a

Index	enVision Name	NetWitness Platform Name	Failure Key
73	[none]	n/a	n/a
74	[none]	n/a	n/a
75	[none]	n/a	n/a
76	[none]	n/a	n/a
77	[none]	n/a	n/a
78	[none]	n/a	n/a
79	[none]	n/a	n/a
80	dmacaddr	eth.dst	n/a
81	smacaddr	eth.src	n/a
82	[none]	n/a	n/a
83	[none]	n/a	n/a
84	[none]	n/a	n/a
85	[none]	n/a	n/a
86	[none]	n/a	n/a
87	[none]	n/a	n/a
[none]	[none]	n/a	n/a
[none]	bytes	bytes	n/a
[none]	packets	packets	n/a
header	[none]	n/a	n/a

Index	enVision Name	NetWitness Platform Name	Failure Key
header	hardware_id	hardware.id	n/a
header	[none]	n/a	n/a
header	[none]	n/a	n/a
header	event_time	event.time	n/a
header	version	version	n/a

November 2020

Trademarks