

ACID: Database (v100-103) ER Diagram

Snort (and other devices) log to database with the following schema:

Snort 1.8 (DB v100-103) and ACID 0.9.6b10 Database ER diagram

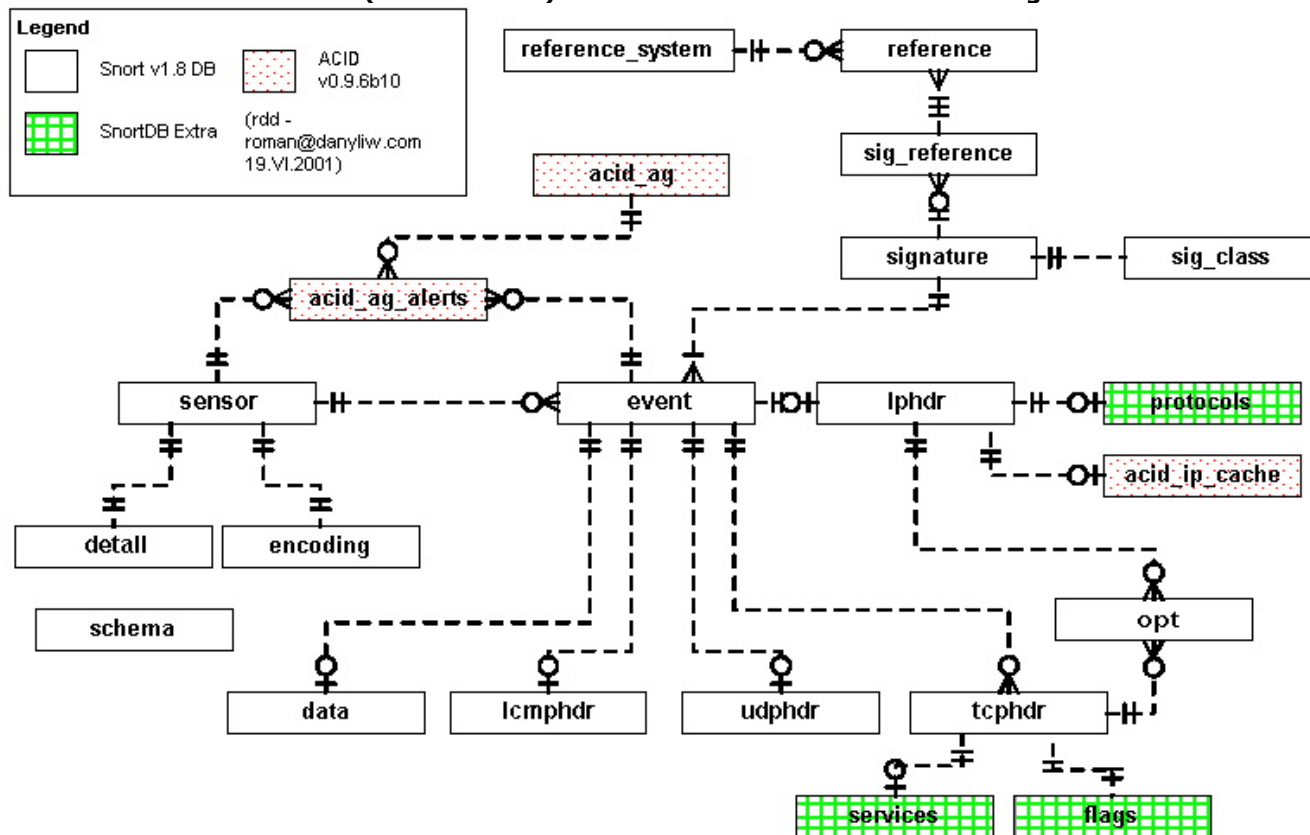


Table	Component	Description
schema	Snort	Self-documented information about the database
sensor	Snort	Sensor name
event	Snort	Meta-data about the detected alert
signature	Snort	Normalized listing of alert/signature names, priorities, and revision IDs
sig_reference	Snort	Reference information for a signature
reference	Snort	Reference IDs for a signature
reference_system	Snort	(lookup table) Reference system list
sig_class	Snort	Normalized listing of alert/signature classifications
data	Snort	Contents of packet payload
iphdr	Snort	IP protocol fields
tcphdr	Snort	TCP protocol fields
udphdr	Snort	UDP protocol fields
lcmphdr	Snort	ICMP protocol fields
opt	Snort	IP and TCP options
detail	Snort	(lookup table) Level of detail with which a sensor is logging
encoding	Snort	(lookup table) Type of encoding used for the packet payload
protocols	SnortDB extra	(lookup table) Layer-4 (IP encoded) protocol list
services	SnortDB extra	(lookup table) TCP and UDP service list
flags	SnortDB extra	(lookup table) TCP flag list
acid_ag	ACID	Meta-data for alert groups
acid_ag_alert	ACID	Alerts in each alert group
acid_ip_cache	ACID	Cached DNS and whois information

schema

Field	Type	Null	Key	Default	Description
vseq	int(10) unsigned		PRI	0	Database schema ID number (e.g. '102')
ctime	datetime			0000-00-00 00:00:00	Timestamp of database creation time

sensor

Field	Type	Null	Key	Default	Description
sid	int(10) unsigned		PRI	NULL	Sensor ID
hostname	text	YES		NULL	Hostname of the sensor (IP if can't qualify)
interface	text	YES		NULL	Network interface (e.g. eth0)
filter	text	YES		NULL	BPF filter
detail	tinyint(4)	YES		NULL	Detail level of the logging
encoding	tinyint(4)	YES		NULL	Encoding format of the payload

event

Field	Type	Null	Key	Default	Description
sid	int(10) unsigned		PRI	0	Sensor ID
cid	int(10) unsigned		PRI	0	Event ID
signature	int(10) unsigned		MUL	0	Signature ID
timestamp	datetime		MUL	0000-00-00 00:00:00	Timestamp of when the event was logged

signature

Field	Type	Null	Key	Default	Description
sig_id	int(10) unsigned		PRI	NULL	Signature ID
sig_name	varchar(255)		MUL		Signature Name
sig_class_id	int(10) unsigned	YES	MUL	NULL	Classification ID
sig_priority	int(10) unsigned	YES		NULL	Priority
sig_rev	int(10) unsigned	YES		NULL	Revision number
sig_sid	int(10) unsigned	YES		NULL	Internal signature ID

sig_reference

Field	Type	Null	Key	Default	Description
sig_id	int(10) unsigned		PRI	0	Signature ID
ref_seq	int(10) unsigned		PRI	0	Reference sequence number (multiple references)
ref_id	int(10) unsigned			0	Reference ID

reference

Field	Type	Null	Key	Default	Description
ref_id	int(10) unsigned		PRI	NULL	Reference ID
ref_system_id	int(10) unsigned			0	Reference system ID
ref_tag	varchar(20)				Reference tag (e.g. CVE-CAN-2001-01)

reference_system

Field	Type	Null	Key	Default	Description
ref_system_id	int(10) unsigned		PRI	NULL	Reference system ID
ref_system_name	varchar(20)	YES		NULL	Reference system name (e.g. CVE)

sig_class

Field	Type	Null	Key	Default	Description
sig_class_id	int(10) unsigned		PRI	NULL	Signature classification ID
sig_class_name	varchar(60)		MUL		Classification name (e.g. recon)

data

Field	Type	Null	Key	Default	Description
sid	int(10) unsigned		PRI	0	Sensor ID
cid	int(10) unsigned		PRI	0	Event ID
data_payload	text	YES		NULL	Packet payload encoded according to sensor.encoding

iphdr

Field	Type	Null	Key	Default	Description
sid	int(10) unsigned		PRI	0	Sensor ID
cid	int(10) unsigned		PRI	0	Event ID
ip_src	int(10) unsigned		MUL	0	Source IP address (32-bit unsigned int)
ip_dst	int(10) unsigned		MUL	0	Destination IP address (32-bit unsigned int)
ip_ver	tinyint(3) unsigned	YES		NULL	IP version
ip_hlen	tinyint(3) unsigned	YES		NULL	IP Header length
ip_tos	tinyint(3) unsigned	YES		NULL	IP type-of-service
ip_len	smallint(5) unsigned	YES		NULL	IP datagram length
ip_id	smallint(5) unsigned	YES		NULL	IP ID
ip_flags	tinyint(3) unsigned	YES		NULL	IP flags
ip_off	smallint(5) unsigned	YES		NULL	IP fragment offset
ip_ttl	tinyint(3) unsigned	YES		NULL	IP time-to-live
ip_proto	tinyint(3) unsigned			0	IP protocol
ip_csum	smallint(5) unsigned	YES		NULL	IP checksum

tcphdr

Field	Type	Null	Key	Default	Description
sid	int(10) unsigned		PRI	0	Sensor ID
cid	int(10) unsigned		PRI	0	Event ID
tcp_sport	smallint(5) unsigned		MUL	0	TCP source port
tcp_dport	smallint(5) unsigned		MUL	0	TCP destination port
tcp_seq	int(10) unsigned	YES		NULL	TCP sequence number
tcp_ack	int(10) unsigned	YES		NULL	TCP ACK number
tcp_off	tinyint(3) unsigned	YES		NULL	TCP offset
tcp_res	tinyint(3) unsigned	YES		NULL	TCP reserved
tcp_flags	tinyint(3) unsigned		MUL	0	TCP flags
tcp_win	smallint(5) unsigned	YES		NULL	TCP window
tcp_csum	smallint(5) unsigned	YES		NULL	TCP checksum
tcp_urp	smallint(5) unsigned	YES		NULL	TCP urgent pointer

udphdr

Field	Type	Null	Key	Default	Description
sid	int(10) unsigned		PRI	0	Sensor ID
cid	int(10) unsigned		PRI	0	Event ID
udp_sport	smallint(5) unsigned		MUL	0	UDP source port
udp_dport	smallint(5) unsigned		MUL	0	UDP destination port
udp_len	smallint(5) unsigned	YES		NULL	UDP length
udp_csum	smallint(5) unsigned	YES		NULL	UDP checksum

icmphdr

Field	Type	Null	Key	Default	Description
sid	int(10) unsigned		PRI	0	Sensor ID
cid	int(10) unsigned		PRI	0	Event ID
icmp_type	tinyint(3) unsigned		MUL	0	ICMP type
icmp_code	tinyint(3) unsigned			0	ICMP code
icmp_csum	smallint(5) unsigned	YES		NULL	ICMP checksum
icmp_id	smallint(5) unsigned	YES		NULL	ICMP ID
icmp_seq	smallint(5) unsigned	YES		NULL	ICMP sequence number

opt

Field	Type	Null	Key	Default	Description
sid	int(10) unsigned		PRI	0	Sensor ID
cid	int(10) unsigned		PRI	0	Event ID
optid	int(10) unsigned		PRI	0	Option ID (multiple options per alert)
opt_proto	tinyint(3) unsigned			0	Option protocol (IP, TCP)
opt_code	tinyint(3) unsigned			0	Option code
opt_len	smallint(6)	YES		NULL	Option length
opt_data	text	YES		NULL	Option data

acid_ag

Field	Type	Null	Key	Default	Description
ag_id	int(10) unsigned		PRI	NULL	Alert Group (AG) ID
ag_name	varchar(40)	YES		NULL	AG name
ag_desc	text	YES		NULL	AG description
ag_ctime	datetime	YES		NULL	Timestamp of AG creation time
ag_ltime	datetime	YES		NULL	Timestamp of last AG modification

acid_ag_alert

Field	Type	Null	Key	Default	Description
ag_id	int(10) unsigned		PRI	0	Alert Group (AG) ID
ag_sid	int(10) unsigned		PRI	0	Sensor ID
ag_cid	int(10) unsigned		PRI	0	Event ID

acid_ip_cache

Field	Type	Null	Key	Default	Description
ipc_ip	int(10) unsigned		PRI	0	IP address (32-bit unsigned int)
ipc_fqdn	varchar(50)	YES	MUL	NULL	FQDN
ipc_dns_timestamp	datetime	YES		NULL	DNS lookup timestamp
ipc_whois	text	YES		NULL	whois information
ipc_whois_timestamp	datetime	YES		NULL	whois lookup time