APFS Reference Sheet

By Jonas Plum and Andreas Dewald

Object

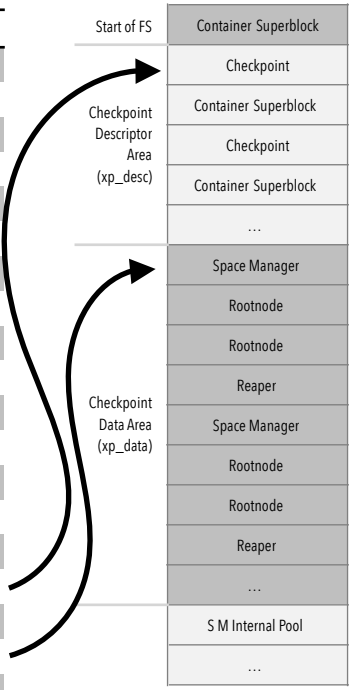
pos	size	type	id
0	8	u8le	cksum
8	8	u8le	oid
16	8	u8le	xid
24	2	u2le	type
26	2	u2le	flags
28	2	u2le	subtype
30	2	u2le	padding

Types:
0x1 Container S.block
0x2 Rootnode
0x3 Node
0x5 Space Manager
0x7 S. M. Internal Pool
0xB B-Tree
0xC Checkpoint
0xD Volume S.block
0x11 Reaper

Subtypes:
0x0 No Subtype
0x9 History
0xB Location
0xE Files
0xF Extents
0x10 Unknown

Container Superblock

pos	size	typ	id
0	4	str	magic 'NXSB'
4	4	u4le	block_size
8	8	u8le	block_count
16	8	u8le	features
24	8	u8le	read_only_compatible_featur
32	8	u8le	incompatible_features
40	16		uuid
56	8	u8le	next_oid
64	8	u8le	next_xid
72	4	u4le	xp_desc_blocks
76	4	u4le	xp_data_blocks
80	8	u4le	xp_desc_base
88	8	u4le	xp_data_base
96	4	u4le	xp_desc_len
100	4	u4le	xp_data_len
104	4	u4le	xp_desc_index
108	4	u4le	xp_desc_index_len
112	4	u4le	xp_data_index
116	4	u4le	xp_data_index_len
120	8	u8le	spaceman_oid
128	8	u8le	omap_oid
136	8	u8le	reaper_oid
152	4	u4le	max_file_systems
160	8	u8le	fs_oid



Ressources:

- Enhanced APFS analysis: Whitepaper by J. Plum and A. Dewald
- Decoding the APFS file system: Paper by K. H.Hansen and F. Toolan in Digital Investigation
- Apple File System Guide: Official documentation on APFS

Last updated: 2018-03-27

Volume Superblock

pos	size	typ	id
0	4	str	magic 'APSB'
4	4	u4le	fs_index
24	4	u4le	features
40	8	u4le	fs_reserve_block_count
48	8	u4le	fs_quota_block_count
56	8	u4le	fs_alloc_count
96	8	u8le	omap_oid
104	8	u8le	root_tree_oid
112	8	u8le	extentref_tree_oid
120	8	u8le	snap_meta_tree_oid
144	8	u8le	next_doc_id
152	8	u8le	num_files
160	8	u8le	num_directories
168	8	u8le	num_symlinks
176	8	u8le	num_other_fsobjects
184	8	u8le	num_snapshots
208	16		vol_uuid
224	8	u8le	last_mod_time
232	8	u8le	formatted_by.last_xid
264	32	str	formatted_by.id
272	8	u8le	formatted_by.timestamp
280	8	u8le	modified_by.last_xid
288	32	str	modified_by.id
320	8	u8le	modified_by.timestamp
672	…	str	volname

B-Tree

pos	size	typ	id
0	8	u8le	btree_type
16	8	u8le	root

Space Manager

pos	size	typ	id
0	4	u4le	block_size
4	4	u4le	blocks_per_chunk
8	4	u4le	chunks_per_cib
12	4	u4le	cibs_per_cab
16	4	u4le	block_count
20	4	u4le	chunk_count
24	4	u4le	cib_count
28	4	u4le	cab_count
32	4	u4le	entry_count
40	8	u8le	free_count
48	4	u4le	entries_offset
144	8	u8le	prev_sm_internal_pool_block
…	…	u8le	spaceman_internal_pool_blocks

Space Man. Internal Pool

pos	size	type	id
4	4	u4le	entry_count
8	…	SMInternalPoolEntry	entries

Space Manager Internal Pool Entry

pos	size	typ	id
0	8	u8le	bitmap_block_xid
16	4	u4le	bm_block_count
20	4	u4le	bitmap_free_blocks
24	8	u8le	bitmap_block

APFS is Little Endian
Timestamps are nanoseconds starting 1970-01-01

Rootnode & Node

pos	size	type	id
0	2	u2le	node_type
2	2	u2le	level
4	4	u4le	entry_count
10	2	u2le	keys_offset
12	2	u2le	keys_length
14	2	u2le	data_offset
16	8	u8le	meta_entry
24	…	EntryHead	entry_heads
…	…	EntryKey	entry_keys
…	…	EntryValue	entry_values

Entry Head

pos	size	typ	id
0	2	s2le	key_offset
2	2	u2le	key_size
4	2	s2le	val_offset
6	2	u2le	val_size

Entry Keys

pos	size	typ	id
0	8	u8le	kind & obj_id
8	8	u8le	xid
16	…	…	depends on kind

Entry Values

Kinds:
0x0 omap
0x2 lookup
0x3 inode
0x4 xattr
0x5 sibling
0x6 extent_status
0x8 extent
0x9 drec

Pointer Value (when node_type is 2)

pos	size	typ	id
0	8	u8le	pointer

xattr value

pos	size	typ	id
0	2	u2le	xattr_obj_id
2	2	u2le	xdata_len
4	…		dstream

omap value

pos	size	typ	id
0	4	u4le	paddr
4	4	u4le	size
8	8	u8le	obj_id

Extent Value

pos	size	typ	id
0	4	u4le	paddr
4	4	u4le	size
8	8	u8le	obj_id

Inode Value

pos	size	type	id
0	8	u8le	parent_id
8	8	u8le	file_id
16	8	u8le	creation_timestamp
24	8	u8le	modified_timestamp
32	8	u8le	changed_timestamp
40	8	u8le	accessed_timestamp
48	8	u8le	flags
56	4	u4le	nchildren_or_nlink
68	4	u4le	bsd_flags
72	4	u4le	owner_id
76	4	u4le	group_id
80	2	u2le	mode
92	2	u2le	xf_num_ext
94	2	u2le	xf_used_data
96	…	xf_hea	xf_header
…	…	xf_field	xfields

Extended Field Header (xf_header)

pos	size	type	id
0	2	u2le	type
2	2	u2le	length

Extended Field Types
0x204 name (string)
0x2008 size (u8le)