Appendix: List of events which Linux Kernel State Tracer records on IA32

Copyright (C) Hitachi, Ltd., 2002-2003. All rights reserved Version 2.03 Categoly Mnemonic Description of events data recorded as "log_arg1 data recorded as "log_arg2 data recorded as "log_arg3" data recorded as "log_arg4" from log arg3, log arg4, can determain prev. process count (value before ddress of the task struc address of the task struc prev. process state (value after rocess context switching 01 ROCESS CONTEXTSWIT schedule(ernel/sched.c witch) vhy processes were switched of "prev" ralue of "p" in the function WAKEUP ROCESS WAKEL try to wake up(value of "sig" in the function value of "fn" in the function Process OCESS_SIGSEND OCESS_LTHREADGEN specific_send_sig_info() alue of "t" in the function pointer to info (info) ending signal creating a kernel thread kernel_thread() ./arch/i386/kernel/process.c pointer to argument of kernel thread (arg) init_waitqueue_head() initialize wait gueue head ointer to wait gueue head ointer to call address ./include/linux/wait.h add_wait_queue(), add_wait_que nter to wait_queue_hea nter to added proces ROCESS REM WQ remove from waitqueue __remove_wait_queue() do_IRQ() inter to wait queue head pinter to removed process INT_HARDWARE_ENTRY INT_TASKLETHI_ENTRY entrance /arch/i386/kernel/irq.c terrupt status (status) pointer to register stack kernel/softirq.c rrupts oftware alue of "t->func" in the function T TASKLET ENTRY entrance tasklet action() address of action (bh base alue of "nr" in the function int3 bounds invalid_op double_fault coprocessor_segment_overrun invalid_TSS segment_not_present rror_code andler address (edi) error code (esi) xception occurred address (eip) stack_segment alignment_check 20 EXCEPTION_ENTRY coprocessor_error simd_coprocessor_ Exceptions /arch/i386/kernel/entry S general_protection page_fault machine_check device not available device not available he number of this exception device_not_available device_not_available handler address EXCEPTION EXIT 21 he number of this exception cording arguments of system calls is 30 SYSCALL ENTRY arch/i386/k<u>ernel/entry.S</u> eginning of system_call() e number of this system call SYSCALL_EXIT ne number of this system call ending of system_call() stem calls ecording arguments of system calls is 32 SYSCALL SYSENTER arch/i386/kernel/entry.S e number of this system call optional feature SCALL SYSEXI sysexit instruction exit ending of sysenter entry() ./arch/i386/kernel/entry.S the number of this system call swap out try_to_swap_out(inter to page swapped out (page /mm/vmscan.c swap in do_swap_page() /mm/memory.c inter to page swapped in (page) MEM_DO_NOPAG MEM_DO_WPPAG ointer to page allocated (new_page)
ointer to page (new page) em do nopage exit nem_do_wppage do_wp_page() ./mm/memory.c entrance exit exit MEM WAIT PAGE nem wait page wait on page(/mm/filemap.c ter to page (page EM_WAIT_FAGE EM_GET_FREEPAGI EM_FREEPAGE ointer to page (paddr the number of page (order call address em_get_freepage _get_free_page(/mm/page_alloc. ointer to page (address ointer to (addr) address (addr) nem get zeropage get zeroed page() /mm/page alloc.c entrance exit nem freepage he number of page (order) call address MEM_VMALLOC MEM VFREE nem vfree entrance nm/vmalloc.o address (addr MEM_CACHE_CREAT MEM_CACHE_ALLOC kmem_cache_create(kmem_cache_alloc() mem_cache_create mem_cache_alloc exit achep mm/slab.c mem_malloc mem_cache_free cachep MEM MALLO kmalloc() call address kmem_cache_free() mm/slab.c entrance MEM FREE mem free entrance /mm/slab.c call address sending packets dev_queue_xmit interrupt on sending packet entrance net tx action() ./net/core/dev. ET_PKTRECV ET_PKTRECV net_rx_action() interrupt on receiving packets entrance NET SOCKETIF socket() entrance sys socketcal ./net/socket.c exit is recorded as exit of system call. /ipc/sem.c sys_semget(argument for the function sys_semctl() sys_msgsend(emnum sys_msgrcv() sys_msgget() msqid/msgflg msgsz msgtyp SYSV_IPC_MSGRCV SYSV_IPC_MSGGET SYSV_IPC_MSGCTL SYSV_IPC_SHMAT /ipc/msg.c PC functions entrance sys_msgctl(sys_shmat() sys_shmdt() shmaddr shmflg raddr hmaddr /ipc/shm.c sys_shmget() shmfla spin_lock() ddress where it was called LK_SPINTRYLOCK
LK_SPINUNLOCK pin lock try lock (exit) spin_trylock() ddress where it was called return value inline unlock write lock write try lock (e write unlock dress where it was called spin_unlock() write_lock() ress where it was calle /include/asm-i386/spinlock.h write_trylock(write_unlock(dress where it was called return value inline K_WRUNLOCK K RDLOCK read lock read lock() ldress where it was called inline read unlock define argument for the function(data) run timer list TIMER_ADD TIMER_MOD function address (timer->function) argument for the function (timer add_timer() inter to timer list (time modify timer list mod_timer() unexpired term (timer->expires) function address (timer->function) argument for the function (timer-TIMER_DEL TIMER_DEL_SYNC OOPS_PGFAULT unexpired term (timer->expires) delete from timer list del timer() pinter to timer list (timer) function address (timer->function) argument for the function (timerfunction address (timer->function) argument for the function (timer delete from timer list with synchronous nter to timer list (timer) a4 unexpired term (timer->expires) oops in page fault handler just before the oops operation do page fault(/arch/i386/mm/fault.c ddress where it was accesse ddress where exception occurre exception error code Oops iust before the oops oper OOPS NMIWDO ddress where it was runn OUT1() and 90 O PORTIN _OUT2() tail of __IN() commands port output /include/asm-i386/io.h ort address/byte width alue to output address where it was called inline O_PORTOUT ort address/byte wid value to input /kernel/panic.o ddress of argumen address where it was called Progress of LKST initialization process lkst_init_stage[0-1]() f00 f01 LKST KERNEL DUMP driver/lkst/lkst_core.c ernel dump event st_dump_notify_handler() an't handle it. ump device f08 LKST switches the masksets Ikst evhandlerprim maskset xchq ./driver/lkst/lkst_core.c old maskset ID pointer to old maskse poniter to new maskse Recorded 2 times; before/after new buffer ID LKST BLIFF SHIFT LKST shifts the buffers lkst evhandlerprim buffer shift in pointer to old buffer f11 LKST_BUFF_OVFLOW errun occurred in the current buffer. lkst_evhandlerprim_entry_next() inlude/linux/lkst_private.h inter to the buffer f masked, LKST stops it. f19 Synchronization with UID sys_*uid(), set_user() /kernel/timer.c, sys.c pointer to the process table for compensation of dropped log data ynchronization with G /kernel/timer.c, sys.c pointer to the process table or compensation of dropped log data ST_SYNC_PGID ST_SYNC_TID synchronization with PG pointer to the process table sys_*pgid(), sys_setsid() or compensation of dropped log data ernel/sys.c f1c Synchronization with TID sys_gettid() /kernel/timer.c, sys.c ID(pid) pointer to the process table for compensation of dropped log data LKST_EXTEND extra argument 1 extra argument 2 extra argument 4 extra argument 3 ffd LKST EXTENDE nd of Extra arguments xtra argument 1 extra argument 3 ./driver/lkst/lkst_device.c LKST_BUFF_OVWRTN lkst_buffer_entry_read_core() for detection of overwritten Overwritten occured while reading LKST ETYPE MAX

		vents which Linux Kernel State	Tracer records on IA64						G :1.	C) II: 1: 1: 1: 1 2002 2002 AII :	1.
Event type [hex]	Version 2.03 Categoly	Mnemonic	Descriptio	on of events	where to hook	filename	data recorded as "log_arg1"	data recorded as "log_arg2"	data recorded as "log_arg3"	C) Hitachi, Ltd., 2002-2003. All ris data recorded as "log_arg4"	hts reserved. Iremarks
01	- canagany	PROCESS_CONTEXTSWITCH	,		schedule()	./kernel/sched.c	address of the task_struct	address of the task_struct	prev. process state (value after	prev. process count(value before	from log_arg3, log_arg4, can determain
		PROCESS WAKEUP	WAKEUP		v	./keme/scried.c	of "prev" value of "p" in the function	of "next" synchronous	switch)	switch)	why processes were switched
02 03	Process	PROCESS_SIGSEND sending signal		try_to_wake_up() specific send sig info()	./kernel/signal.c	value of "sig" in the function	value of "t" in the function	pointer to info (info)			
04	management	PROCESS_LTHREADGEN	OCESS_LTHREADGEN creating a kernel thread		kernel_thread()	./arch/ia64/kernel/process.c	value of "fn" in the function	pointer to argument of kernel thread (arg)	flag		
05		PROCESS_INIT_WQH PROCESS ADD WQ			init_waitqueue_head()	./include/linux/wait.h	pointer to wait_queue_head	pointer to call address pointer to added process			
06 07		PROCESS_ADD_WQ PROCESS REM WQ	remove from waitqueue		add_wait_queue(),add_wait_queue remove_wait_queue()	./include/iinux/wait.n	pointer to wait_queue_head pointer to wait_queue_head	pointer to added process pointer to removed process			
10	10 12 14 Interrupts	INT_HARDWARE_ENTRY		entrance	do_IRQ()	./arch/ia64/kernel/irq.c	value of "irq" in the function	interrupt status (status)	pointer to register stack		
12		INT_TASKLETHI_ENTRY	a of the same	entrance	tasklet_hi_action()	./kernel/softirq.c	value of "t->func" in the function				
16		INT_TASKLET_ENTRY INT_BH_ENTRY	software	entrance entrance	tasklet_action() bh action()	1	value of "t->func" in the function value of "nr" in the function	address of action (bh_base)		+	
	EXCEF EXCEF EXCEF EXCEF		vhpt_miss					(5.2.55)			
20		EXCEPT_PGFLT_ENTRY	dtlb_miss alt_itlb_miss	entrance		./arch/ia64/mm/fault.c					
					ia64_do_page_fault()		fault address(ifa) is	isr	ipsr	iip	
21				exit							
		EVOCET III OR ENTEN	nested_dtlb_miss	entrance							
22		EXCEPT_ILLOP_ENTRY EXCEPT ILLOP EXIT			ia64_illegal_op_fault()		ec		ipsr	iip	
24		EXCEPT BADBRK ENTRY	PEDT DADDDY ENTDY		inC4 had break()	_	hand number(iim)		leas	iin.	
25		EXCEPT_BADBRK_EXIT	break_instruction	exit	ia64_bad_break()		break number(iim)		ipsr	пр	
26		EXCEPT_FAULT_ENTRY	nat_consumption debug_vector unsupported_data_reference fp_fault fp_trap lower_privilege_transfer_trap taken_branch_trap single_step_trap ia32_exception la32_interrupt	entrance		./arch/ia64/kernel/traps.c	fault vector number	isr	ipsr	iip	
					-ia64_fault()						
27		EXCEPT_FACET_EXIT		exit							
28		EXCEPT_UNALIGN_ENTRY		entrance	ia64_handle_unaligned()	./arch/ia64/kernel/unaligned.c	ifa		insr	iin	
29		EXCEPT_UNALIGN_EXIT		exit		-	ovetom cell function address	the number of this quotom sall	ipo.	''P'	recording arguments of system calls is
30 31	System calls	SYSCALL_ENTRY SYSCALL EXIT	entrance exit		beginning of system_call() ending of system_call()	./arch/ia64/kernel/ivt.S	system call function address system call function address	the number of this system call errno			recording arguments of system calls is optional feature
50		MEM_SWAPOUT	swap out	exit	try_to_swap_out()	./mm/vmscan.c	pointer to page swapped out (page)				
51	Memory Management	MEM_SWAPIN	swap in	exit	do_swap_page()	./mm/memory.c	pointer to page swapped in (page)				
52 53		MEM_DO_NOPAGE MEM DO WPPAGE		exit	do_no_page()	./mm/memory.c ./mm/memory.c	pointer to page (new page)			 	
53 54		MEM_DO_WPPAGE MEM_WAIT_PAGE	mem_do_wppage mem_wait_page	entrance	do_wp_page() wait_on_page()	./mm/memory.c ./mm/filemap.c	pointer to page (new page) pointer to page (page)			1	
55		MEM_GET_FREEPAGE	mem_get_freepage	exit	_get_free_page()	./mm/page_alloc.c	pointer to page (paddr)	type of page (gfp_mask)	the number of page (order)	call address	
56 57		MEM_GET_ZEROPAGE	mem_get_zeropage	exit	get_zeroed_page()	./mm/page_alloc.c	pointer to page (address)	type of page (gfp_mask)	call address		
57 58		MEM_FREEPAGE MEM_VMALLOC		entrance exit	free_pages() vmalloc()	./mm/page_alloc.c ./mm/vmalloc.h	pointer to (addr) address (addr)	the number of page (order)	call address call address	+	
59		MEM_VFREE	mem_vfree	entrance	vfree()	./mm/vmalloc.c	address (addr)			<u> </u>	
5a		MEM_CACHE_CREATE	mem_cache_create	exit	kmem_cache_create()	./mm/slab.c	name	size	cachep		
5b 5c		MEM_CACHE_ALLOC MEM_MALLOC		exit exit	kmem_cache_alloc() kmalloc()	./mm/slab.c ./mm/slab.c	cachep cachep	flags	objp objp	call address	
50 5d		MEM_MALLOC MEM CACHE FREE		entrance	kmem_cache_free()	./mm/slab.c	cachep	flags objp	call address	ouii auuress	
5e		MEM_FREE	mem_free	entrance	kfree()	./mm/slab.c	objp	call address			
60		NET_PKTSEND	sending packets	entrance	dev_queue_xmit()	./net/core/dev.c	skb				
61 62	Networking	NET_PKTSENDI NET PKTRECV	interrupt on sending packets receiving packets	entrance entrance	net_tx_action() netif rx()	./net/core/dev.c	n Iskb				
63		NET_PKTRECVI	interrupt on receiving packets	entrance	net_rx_action()	./net/core/dev.c	h				
64	Ī	NET_SOCKETIF	socket()	entrance	sys_socketcall	./net/socket.c	call	args			exit is recorded as exit of system call.
70 71	SysV IPC	SYSV_IPC_SEMOP SYSV_IPC_SEMGET	IPC functions		sys_semop() sys_semget()	./ipc/sem.c ./ipc/msg.c ./ipc/shm.c	semid key	tsops nsems	nsops semflq		
72		SYSV_IPC_SEMGET		entrance	sys_semiget() sys_semctl()		semid	semnum	cmd	argument for the function (arg. pad)	
73		SYSV_IPC_MSGSEND			sys_msgsend()		msqid	msgp	msgsz	msgflg	
74 75		SYSV_IPC_MSGRCV			sys_msgrcv()		msqid/msgflg	msgp	msgsz	msgtyp	
75 76		SYSV_IPC_MSGGET SYSV_IPC_MSGCTL			sys_msgget() sys_msgctl()		msaid	msgflg cmd	buf	+	
77		SYSV IPC SHMAT			sys_shmat()		shmid	shmaddr	shmflg	raddr	
78		SYSV_IPC_SHMDT			sys_shmdt()		shmaddr				
79		SYSV_IPC_SHMGET SYSV_IPC_SHMCTL			sys_shmget() sys_shmctl()		key shmid	size cmd	shmflg buf		
7a 80	Locks	LK_SPINLOCK		lock	spin_lock()		address where it was called	lock		1	inline
81		LK_SPINTRYLOCK	spin lock	try lock (exit)	spin_trylock()		address where it was called	lock	return value		inline
82 83		LK_SPINUNLOCK LK WRLOCK		unlock write lock	spin_unlock() write lock()	./include/asm-ia64/spinlock.h	address where it was called address where it was called	lock rwlock		-	inline inline
84		LK_WRTRYLOCK	read/write lock	write try lock (exit)	write_trylock() (IA32 only)		address where it was called	rwlock	return value		inline
85		LK_WRUNLOCK		write unlock	write_unlock()		address where it was called	rwlock			define
86 87		LK_RDLOCK LK_RDUNLOCK		read lock read unlock	read_lock() read_unlock()		address where it was called address where it was called	rwlock rwlock			inline define
a0		TIMER_RUN	run timer list	rodu urilook	run_timer_list()		function address(fn)	argument for the function(data)		<u>† </u>	
a1		TIMER_ADD	add to timer list		add_timer()		pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	argument for the function (timer-	
a2		TIMER_MOD	modify timer list		mod_timer() del timer()	./kernel/timer.c	pointer to timer list (timer) pointer to timer list (timer)	unexpired term (timer->expires) unexpired term (timer->expires)	function address (timer->function) function address (timer->function)	argument for the function (timer- argument for the function (timer-	
<u>a3</u> a4		TIMER_DEL TIMER_DEL_SYNC	delete from timer list delete from timer list with synchror	nous	del_timer_sync()	1	pointer to timer list (timer) pointer to timer list (timer)	unexpired term (timer->expires) unexpired term (timer->expires)	function address (timer->function) function address (timer->function)	argument for the function (timer- argument for the function (timer-	
				port input	ia64_inb() ia64_inw()			((argument for the function (unter	
90		O_PORTIN	io commands		ia64_inl() ia64_insb()		port address/byte width	value to input	address where it was called		inline
					ia64_insw()	./include/asm-ia64/io.h					
]				ia64_insl()						
	Others			port input	ia64_outb()		port address/byte width	value to output	address where it was called		
		0. 000701:-			ia64_outw() ia64_oul()						
91		O_PORTOUT			ia64_outsb()						inline
					ia64_outsw()						
92		O PANIC	panic		ia64_outsl() panic()	./kernel/panic.c	address of argument	address where it was called			
93		O_PRINTK	printk		printk()	./kernel/printk.c	address of argument	address where it was called		<u> </u>	
b0	Oops	OOPS_PGFAULT		just before the oops operation	do_page_fault()	./arch/ia64/mm/fault.c	address where it was accessed	address where exception occurred	exception error code		
f00 f08	LKST Linternal event L	LKST_INIT LKST MSET XCHG	Progress of LKST initialization pro- LKST switches the masksets	ocess	lkst_init_stage[0-1]()	./driver/lkst/lkst_core.c	initialization status old maskset ID	new macked ID	pointer to old masksat	popitar to new maskest	Recorded 2 times: hotoro/cfts-
f10		LKST_MSET_XCHG LKST_BUFF_SHIFT	LKST switches the masksets LKST shifts the buffers		<pre>lkst_evhandlerprim_maskset_xchg_inline lkst_evhandlerprim_buffer_shift_inline()</pre>		old maskset ID old buffer ID	new maskset ID new buffer ID	pointer to old maskset pointer to old buffer	poniter to new maskset pointer to new buffer	Recorded 2 times; before/after Recorded 2 times; before/after
		ST_BUFF_OVFLOW overrun occurred in the current buff			omana.orpiini_bunoi_ariiit_inilile()		5.5 54.01.15			- I I I I I I I I I I I I I I I I I I I	Used for automatically shifting buffer.
f11				iffer.	lkst_evhandlerprim_entry_next()		pointer to the buffer			If masked, LKST stops it.	
f19		LKST_SYNC_UID	Synchronization with UID		sys_*uid(), set_user() . sys_*gid() .	./kernel/timer.c, sys.c	UID		pointer to the process table		for compensation of dropped log data
f1a		LKST_SYNC_GID	Synchronization with GID			./kernel/timer.c, sys.c	GID	DCDD	pointer to the process table	cossion loader flee	for compensation of dropped log data
f1b f1c		LKST_SYNC_PGID LKST_SYNC_TID	D Synchronization with TID Extra arguments E End of Extra arguments		sys_*pgid(), sys_setsid() sys_gettid()	./kernel/sys.c ./kernel/timer.c, sys.c	PID TID(pid)	PGRP	pointer to the process table pointer to the process table	session leader flag	for compensation of dropped log data for compensation of dropped log data
ffc		LKST_SYNC_TID LKST_EXTEND			Joyo_gettiu()	., nomerumet.c, sys.c	extra argument 1	extra argument 2	extra argument 3	extra argument 4	ror compensation or dropped log data
ffd		LKST_EXTENDE					extra argument 1	extra argument 2	extra argument 3	extra argument 4	
ffe		LKST_BUFF_OVWRTN	Overwritten occured while reading)	lkst_buffer_entry_read_core()	./driver/lkst/lkst_device.c					for detection of overwritten
fff		LKST_ETYPE_MAX	Maximum event number								limitation value.
				· · · · · · · · · · · · · · · · · · ·							· · · · · · · · · · · · · · · · · · ·