A APPENDIX

A.1 More Graphs for § 5.1

Figure 8 shows how existing auditing frameworks drop events with different hardware configurations other than those in Section 5.1. It also shows that NODROP does not drop any events. This result is consistent with the conclusion in Section 5.1.

A.2 More Graphs for § 5.2

Figure 9, Figure 10 and Figure 11 show the Nginx, Redis, and OpenSSL results respectively. Note that for all three figures, subfigure (a)-(h) represent configurations of 1 CPU core with 2GB memory, 4 CPU cores with 8GB memory, 16 CPU cores with 32GB memory, and 32 CPU cores with 64 GB memory on both virtual and physical machine respectively. Overall, existing auditing frameworks can substantially slow down other applications when the super producer's workload increases. The Figures also show that NODROP does not slow other applications. These results are consistent with the conclusion in Section 5.2.

A.3 More Results for § 5.3.1

Table 6 shows the performance scores of `lmbench` for other hardware configurations besides those in § 5.3.1. Overall, the conclusion is consistent with § 5.3.1.

Table 6: Performance scores of `lmbench`. *Values are shown as percentages relative to Sysdig. The negative value means* NODROP *is faster than Sysdig.*

Configurations	C1	C2	C3	C4	Ave
Syscall Tests					
NULL syscall	-11.2%	-18.0%	-13.2%	-8.1%	-12.6%
stat	-4.4%	+9.1%	-0.0%	+1.2%	-3.1%
fstat	+5.4%	+4.0%	-1.2%	+3.2%	+2.9%
open/close file	-0.5%	-8.0%	-0.9%	-3.0%	-3.1%
read file	-0.5%	+3.0%	+5.9%	+5.9%	+3.6%
write file	+1.5%	+2.7%	+6.0%	+6.9%	+4.3%
File Access					
file create (0K)	+2.1%	+7.6%	-0.7%	+0.3%	+2.4%
file delete (0K)	-2.5%	-2.0%	-0.5%	0.0%	-1.3%
file create (10K)	-4.4%	+1.6%	-1.2%	-1.2%	-1.3%
file delete (10K)	-4.1%	-2.9%	-0.3%	+0.2%	-1.8%
pipe	+0.5%	-3.8%	+7.0%	+7.0%	+2.7%
AF_UNIX	-6.3%	-8.6%	+8.5%	+9.0%	+0.6%

A.4 More Results for § 5.3.2

Table 7a and Table 7b show the application benchmark results for other hardware configurations besides those in § 5.3.2. On average, the application overhead of NODROP is smaller than that of Sysdig. The conclusion in this section is also consistent with the conclusion in § 5.3.2.

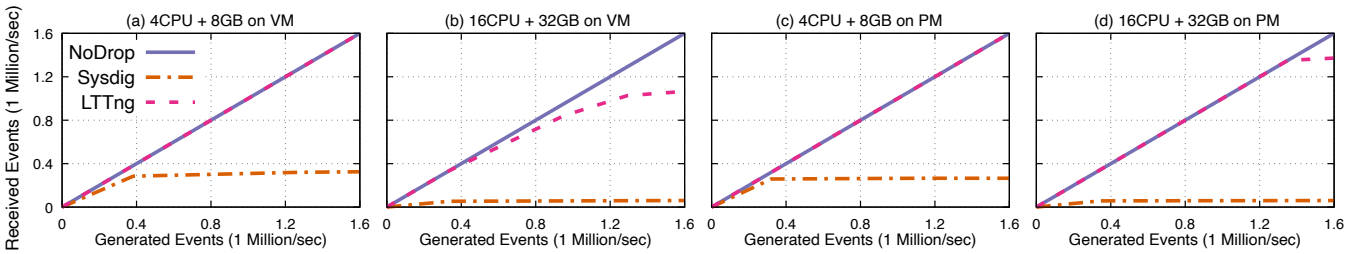

Figure 8: The number of events dropped by NODROP and baselines with different hardware configurations. The x-axis is the number of generated events in 30 seconds, the y-axis is the number of events handled by the auditing framework.

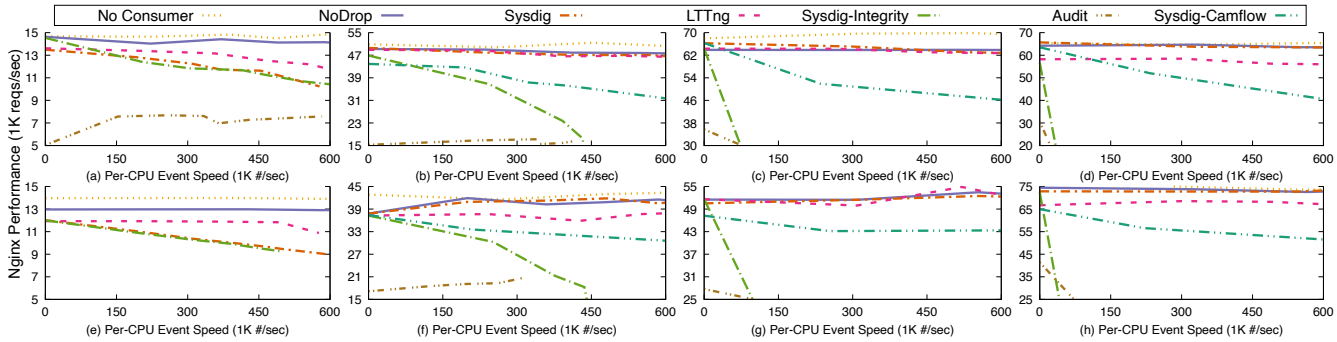

Figure 9: The performance of Nginx on different platforms with different workloads from the super-producer on platforms with different hardware configurations. The x-axis is the speed of generated events in 30 seconds, thy-axis is the performance score of Nginx, measured in the number of requests per second.

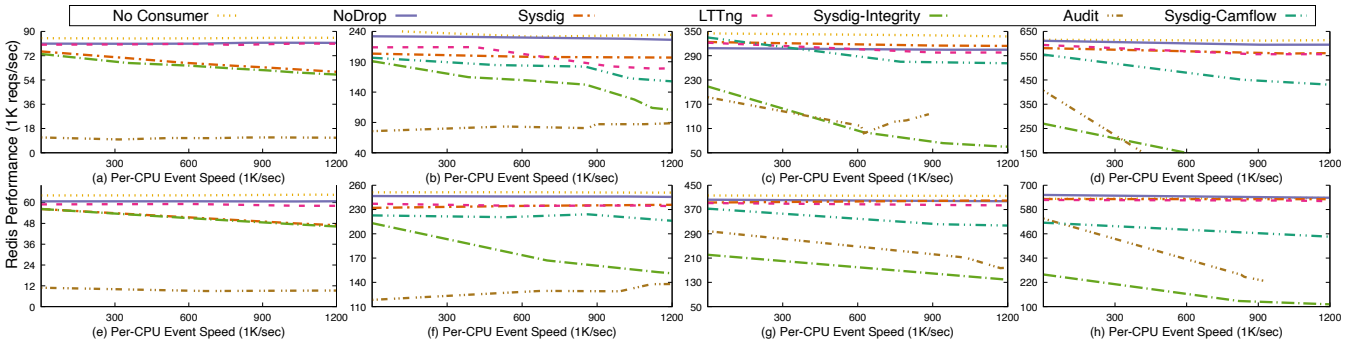

Figure 10: The performance of Redis on different platforms with different workloads from the super-producer on platforms with different hardware configurations. The x-axis is the speed of generated events in 30 seconds, the y-axis is the performance score of Redis, measured in the bandwidth.

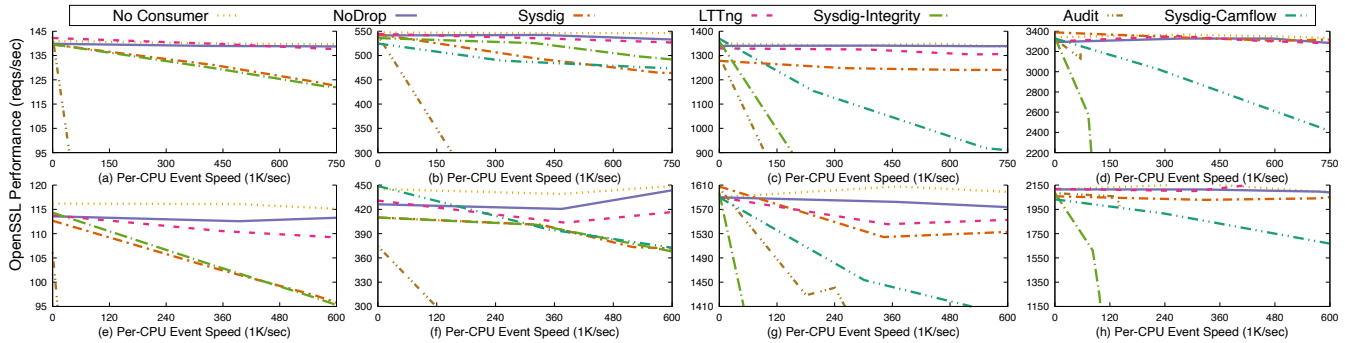

Figure 11: The performance of OpenSSL on different platforms with different workloads from the super-producer on platforms with different hardware configurations. The x-axis is the speed of generated events in 30 seconds, the y-axis is the performance score of OpenSSL, measured in the number of requests per second.

(a) **Benchmark WITHOUT super producer.**

Application	Collector	C2	C3	C6	C7
Nginx	Nodrop	5.00	2.40	8.84	3.37
	Sysdig	16.30	12.10	21.20	9.50
	DIFF	**-9.70**	**-8.60**	**-10.20**	**-5.60**
Redis	Nodrop	6.40	7.40	4.18	11.79
	Sysdig	14.10	13.50	16.40	15.60
	DIFF	**-9.00**	**-7.10**	**-10.50**	**-3.30**
Postmark	Nodrop	28.20	20.20	35.77	27.57
	Sysdig	23.20	18.40	23.20	16.50
	DIFF	**4.10**	**1.50**	**10.20**	**9.50**
Django (Python)	Nodrop	1.60	1.00	1.60	0.50
	Sysdig	1.20	0.20	1.40	0.10
	DIFF	0.50	0.80	0.20	0.40
http (Golang)	Nodrop	6.20	2.40	6.19	4.20
	Sysdig	10.60	4.40	11.90	4.10
	DIFF	**-4.00**	**-1.80**	**-5.10**	0.10
OpenSSL	Nodrop	1.00	0.10	0.00	1.60
	Sysdig	0.40	0.50	0.20	1.70
	DIFF	0.60	-0.30	-0.20	-0.10
7-ZIP	Nodrop	1.20	0.40	0.80	1.10
	Sysdig	0.70	0.30	1.00	0.80
	DIFF	0.50	-0.10	-0.20	0.30
PostgreSQL	Nodrop	6.40	4.72	8.80	6.10
	Sysdig	10.70	8.30	10.30	7.80
	DIFF	**-4.04**	**-3.40**	**-1.30**	**-1.60**

(b) **Benchmark WITH super producer.**

C2	C3	C6	C7
5.10	7.80	4.34	7.99
13.50	12.76	10.30	11.10
-7.40	**-4.40**	**-5.40**	**-2.80**
2.30	1.30	1.25	0.28
21.07	8.00	10.90	3.70
-15.50	**-6.20**	**-8.70**	**-3.30**
22.10	39.90	20.30	35.50
4.54	17.66	8.77	18.44
16.80	**18.90**	**10.60**	**14.40**
1.50	1.70	1.60	2.20
3.15	0.20	1.80	1.09
-1.60	**1.50**	-0.20	**1.10**
3.60	4.50	7.30	4.20
2.47	1.65	6.45	1.26
1.10	**2.80**	**0.80**	**2.90**
2.60	0.47	2.81	1.35
21.71	13.91	22.10	9.10
-15.70	**-11.80**	**-15.80**	**-7.10**
0.90	1.30	0.70	0.90
16.38	6.74	15.22	6.32
-13.30	**-5.10**	**-12.60**	**-5.10**
9.40	7.30	10.70	8.90
13.38	7.94	13.20	9.32
-3.60	-0.59	**-2.20**	-0.38

Table 7: **We measured the processing time per request/transaction for seven representative applications and a Kubernetes-based PostgreSQL. For each application, the first two lines show the relative runtime overhead (%) compared to vanilla Linux, where a lower value indicates performance closer to that of vanilla Linux. The third line shows the relative overhead between Nodrop and Sysdig, with values smaller than 0 indicating that NODROP outperforms Sysdig. For brevity, we denote this as DIFF. We report the mean values across 10 runs, with p-values less than 0.05 shown in bold.**