∂TRIUMF

Canadian ATLAS Tier-1 Analytics Infrastructure

Fernando Fernandez Galindo TRIUMF Scientific Computing Department ATLAS Tier-1 Group

HEPiX Autumn 2023 Workshop October 16-20, 2023



1

ANALYTICS PROJECT MOTIVATION

500

Is/Pr

- With growing infrastructure an ever-increasing collection of heterogeneous monitoring data is produced.
- Our existing monitoring and alerting implementation is robust and stable but rather static and isolated.
- Early 2020 we started the analytics project on hardware that was deprecated.
- The project's main objectives are:
 - Transform static logs into analyzable data.
 - Create a framework where the different datasets can be brought in together for analysis and monitoring.
 - Experiment with data analysis tools like ML, to assist in finding correlations between different areas of our infrastructure, detect anomalies and inefficiencies.

Nagios Host Group Host Status Summary Service Status Summary Admin Nodes (admin_nodes) Analytics Nodes (analytics nodes Compute 1 Nodes (compute01 nodes Compute 2 Nodes (compute02_nodes Compute 3 Nodes (compute03_nodes) Compute 4 Nodes (compute04_nodes) Compute 5 Nodes (compute05_nodes) Compute 6 Nodes (compute06_nodes Ganglia Compute 7 Nodes (compute07 nodes Compute 8 Nodes (compute08_nodes ATLAS Tier-1 Grid Memory last day ATLAS Tier-1 Grid Load last day 40 20 k 30 15 k Bute 20 T 10 10 T 5 Fri 00:00 Fri 12-0 Fri 00:00 Fri 12:00 Use □ 1-min Min: 9.8k Avg: 10.5k Max: 11 Share Now Now: 10.7k 0.0 Min: 0.0 Max Cache 23.8T Now: Min: 18.7T Max: Nodes Now:276.0 Min:274.1 Avg:275.9 Max:276. Buffer Now: 27.8G Min: 26.3G 50.5G Max: Now: 10.0k Min: 9.9k Avg: 10.0k Max: 10. CPUs Free Now: 1.5T Min: 1.4T Avg 2.0T Max: 4.6T 10.5k Min: 9.7k Avg: 10.3k Max: 10. Now: Now: 466.3G Min: 248.8G Avg: 362.8G Max: 576.8G Now: 37.3T Min: 37.3T Avg: 37.3T Max: ATLAS Tier-1 Grid CPU last day 100 ATLAS Tier-1 Grid Network last day 30 G 20 0 Butes Fri 00:00 Fri 12:00 Max: 54.6% User Now: 53.8% Min: 50.1% Avg: 52.9% 3 3% Avg 4 1% Max: 5 9% Max: 26.1G In Now: 6.4G Min: 1.1G Avg: 7.5G Now 4.2% Min: 3.8% Avg 4.5% Max: 5.5% Out Now: 8.4G Min: 1.6G Avg: 7.8G Max: 23.0G Now 0.5% Min: 0.2% Avg 0.5% Max: 1 6% 0.0% Min: 0.0% Avg: 0.0% Max: 0.0% 0.0% Min: 0.0% Avg: 0.0% Max: 0.0%

Min: 36.6% Avg: 37.9%

Max: 39.1%



SOFTWARE OVERVIEW



All our software is deployed using Ansible.





Logs

S

⊢

S

٩

⊢

4

Service	Size (GB)	Storage DB	Service	Size (GB)	Storage	
dCache (billing,	9,850	Elasticsearch	dCache (queues, movers)	215	Elasticsearch	
ftp srm webdav xrootd access)			dCache (netflows)	110	Elasticsearch	
network (router)	30	Elasticsearch	HTCondor (job history,	32	Elasticsearch	
SNMP (traps)	15	MariaDB	status)			
system (auth, iptables, kernel)	1,000	Elasticsearch	infrastructure (DDN and inlet temps, SSD TBW)	160	Elasticsearch	
			infrastructure (humidity, PDU, temps, etc)	2*	RRD	
ELK Ingestion Rate	9		mySQL (status)	4	Elasticsearch	
Service		events/sec	network (router sflow)	15	influxDB	
Mean		600	postgreSQL (activity,	920	Elasticsearch	
Max		12,000	bgwriter, database)			
			system (cpu, mem, net, etc)	2*	RRD	
			tape library stats (device, volume)	2	influxDB	
			tape library (consumption,	2*	RRD	

staging, etc)

* 2GB for all datasets in RRD

GRAFANA

- Currently using version 10.0.3
- Our main visualization software for the following reasons:
 - It can use a large variety of different data sources.
 - Has many options for creating nice looking dashboards easily.
 - Powerful templating of panels.
 - It can further transform data on the fly.
 - It can generate alerts data query-based alerts.





ELASTIC SUITE

- It is the workhorse of the analytics platform.
- We obtained a trial for the full license to investigate their ML tools but due to technical limitations, we didn't get much out of it. Pricing was very expensive to keep the license.
- We use the free 'basic' license.
- Currently using version 8.3.3.
- Elasticsearch:
 - Flexible database, can hold heterogeneous data.
 - Easy to grow horizontally.
 - Many tools to manage and transform data.



- Logstash:
 - Many filters to parse and enrich data.
 - Multiple instances and pipelines to balance the load.
 - Many input and output protocols.
 - Persistent and 'dead-letter' queues.
- Beats:
 - 'Smart' collectors that monitor log files (Filebeat), service metrics (Metricbeat) and network ports (Packetbeat).
 - Balance loads to multiple outputs and queues data if they are unavailable.



ELK INFRASTRUCTURE



- Data collection consists of Filebeat, Metricbeat and Packetbeat instances installed on each host of interest.
- Data is sent to Logstash for processing before being stored in Elasticsearch.
- The Elasticsearch cluster consists of 9 instances running on VM's.
- Kibana shares a VM and is mostly used for administration of the cluster.

- There are 5 types of Elasticsearch instances:
 - 1x Voting-only Master Node (also running Kibana and main endpoint)
 - 2x Master Nodes.
 - 2x "Hot" Data Nodes (nvme storage)
 - 2x "Warm" Data Nodes (ssd storage)
 - 2x Ingest and Transform Nodes (also running Logstash)



NEW HARDWARE (FALL 2022)

Frontend (Elasticsearch and clients)

- 1x PowerEdge R650
- CPU:

2x Xeon 6336Y – 24 cores with Scikit-learn extensions.

• GPU:

Nvidia Telsa T4

- Memory: 256GB
- Network:

Nvidia Mellanox ConnectX-5

• Storage: 2x 480GB SSD (OS)

2x 3.84TB NVMe

Backend (Elasticsearch and Logstash)

- 2x PowerEdge R650
- CPU: Xeon 6326 – 16 Cores
- **Memory:** 256GB



- Network: Nvidia Mellanox ConnectX-5
- Storage: 2x 480GB SSD (OS)
 2x 3.84TB NVMe (Hot Data)
 2x 7.68TB SSD (Warm Data)
- KVM will be used to create 4 ES nodes: master, hot data, warm data, transform (with Logstash).



ahw-fe01	
analytics	
CPU: 24 GPU: Network: 2x Mellanox VFS (10Gb) Memory: 220GB	
Storage: QCOW2 (from SSD): Roles: - Data 100GB master Kibana NVMe 3.84T x 2	



ahw-	kvm01
es-dat	a-hot01
CPU: 10	Memory: 92GB
Network: 2x Mellanox VFS (10Gb)	Roles: data-content data-hot
Storage: NVMe 3.84T x 2	
es-data	-warm01
CPU: 10	Memory: 80GB
Network: 2x Mellanox VFS (10Gb)	Roles: data-warm
Storage: SSD 7.68TB x 2	
es-m	nain01
CPU: 4	Memory: 8GB
Network: 2x Mellanox VFS (10Gb)	Roles: master
es	tr01
CPU: 8	Memory: 52GB
Network: 2x Melianox VFS (10Gb)	Roles: ingest remote-cluster-client transform Logstash

ahw-	kvm02
es-dat	ta-hot02
CPU: 10	Memory: 92GB
Network: 2x Mellanox VFS (10Gb) Storage:	Roles: data-content data-hot
NVME 3.641 X 2	
es-data	t-Warmuz
CPU: 10	Memory: 80GB
Network: 2x Mellanox VFS (10Gb)	Roles: data-warm
Storage: SSD 7.68TB x 2	
es-n	nain02
CPU: 4	Memory: 8GB
Network: 2x Mellanox VFS (10Gb)	Roles: master
es	-tr02
CPU: 8	Memory: 52GB
Network: 2x Mellanox VFS (10Gb)	Roles: ingest remote-cluster-client transform Logstash



Fernando Fernandez Galindo TRIUMF Scientific Computing Department HEPiX Autumn 2023 Workshop October 16-20, 2023

Data	a Acquisition		Le	gend
Kibana	Clients Grafana Scripts		Tier-1 Internal Network	ES Transport network
	\$	ſ	Data C	Collection
	ES Masters			
Hosts: analytics (voting-only) es-main01 es-main02	2 are required online to reach 'quorum', the cluster goes red and stops receiving data to avoid split- brain.		Data Filebeat Metricbeat	Shippers Packetbeat Scripts
Description: No data storage.	Receive and coordinate data queries.			
These manage and coordinat Elasticsearch cluster.	e the		Data Ma	ar ipulation
			Data Ingestio	n and Transforms
Da	ata Storage		Hosts: es-tr01 es-tr02	and uses Logstash and Elasticsearch Ingest pipelines to extract and enrich raw logs and metrics.
	Hot Data		No permanent data is stored	d, Elasticsearch Transforms are
Hosts: es-data-hot01 es-data-hot02	Stores new raw and aggregated data.		Receive data from collector	aggregations and s summmaries.
Description: Fast NVMe drives.	Main source for 'real-time' data.		An	alytics
			Hosts:	
	Warm Data		Analytics	
Hosts: es-data-warm01 es-data-warm02	Stores data that is considered 'historical'.		Description: Scripts that use data stored order to create statistical	in
Description: SSD drives.	Source/backup for data that cannot be re-created.		models.	

PIPELINE

સ્ટે

Fernando Fernandez Galindo TRIUMF Scientific Computing Department HEPiX Autumn 2023 Workshop October 16-20, 2023

LOGSTASH PIPELINE - PARSING

- 1. Logstash receives data from the beats
- 2. A pipeline name is injected in the configuration specific to each of the different logs.

Example:

- tier1-logs-dcache-billing-log-v4
- 3. Data is parsed into fields for each dataset.
- Enrichment settings are applied, so that the pipeline knows if each of the next steps should be applied or not (shown in the next slide).





LOGSTASH PIPELINE - ENRICHMENT

- URLs parsed into fields for protocol, hostname, path, query.
- 2. Anonymize data (specific to each pipeline).
- 3. Parse addresses and reverse resolve IP's.
- 4. Resolve DNS names.
- 5. Add GeoIP data.
- 6. Add Tier-1 Infrastructure location information (datacenter, rack, row, etc).





LOGSTASH PIPELINE - FINAL STAGE

- Remove unwanted fields like metadata from the Beats or just fields we don't really need.
- 2. Create hash of the original message to use for deduplication and as document ID.
- 3. Output to Elasticsearch.





TOKENIZING - BEFORE

• We are drowned by the details.

• Unique error message count: 3,423

Tier-1 - Logs - dChache - E	illing - Error Messages	(¢
Top 1000 values of \sim	Top 1000 values of error.message.keyword	Count of records $\scriptstyle \checkmark$
10006	Flush was cancelled.	329,292
10006	Stage was cancelled.	130,937
10006	Request to [>PoolManager@dCacheDomain] timed out.	103,987
10006	Failed to select pool: Request to [>PoolManager@dCacheDomain] timed out.	31,541
10006	No connection from client after 300 seconds. Giving up.	13,517
10006	No redirect from mover on pool PoolName=sfa14kx_1_lun8 PoolAddress=sfa14kx_1_lun8@sfa14kx_1_lun8 after 3 min	10,787
10006	No redirect from mover on pool PoolName=sfa14kx_1_lun68 PoolAddress=sfa14kx_1_lun68@sfa14kx_1_lun68 after 3 min	10,437
10006	No redirect from mover on pool PoolName=hsmnostage PoolAddress=hsmnostage@hsmpool14_nostage after 3 min	3,291
10006	No redirect from mover on pool PoolName=hsmpool19_sfa14_2_lun48_2 PoolAddress=hsmpool19_sfa14_2_lun48_2@hsmpool19_sfa14_	2,770
10006	No redirect from mover on pool PoolName=hsmpool19_sfa14_2_lun48 PoolAddress=hsmpool19_sfa14_2_lun48@hsmpool19_sfa14_2_lur	2,715
10006	No redirect from mover on pool PoolName=hsmpool18_sfa14_1_lun48_2 PoolAddress=hsmpool18_sfa14_1_lun48_2@hsmpool18_sfa14_	2,690
10006	No redirect from mover on pool PoolName=sfa14kx_2_lun86 PoolAddress=sfa14kx_2_lun86@sfa14kx_2_lun86 after 3 min	2,404
10006	No redirect from mover on pool PoolName=hsmpool20_sfa14_1_lun50_2 PoolAddress=hsmpool20_sfa14_1_lun50_2@hsmpool20_sfa14_	2,213
10006	No redirect from mover on pool PoolName=sfa14kx_2_lun43 PoolAddress=sfa14kx_2_lun43@sfa14kx_2_lun43 after 3 min	2,050



TOKENIZING

- By "tokenizing" we mean normalizing log messages by applying a placeholder or "token" instead of highly variable data.
- For example, IPs and Hostnames are replaced with "IP" or "HOSTNAME" or in dCache cell names are replaced with "CELL_NAME".
- Therefore, we get the base error message which can then be aggregated, used in statistics, clean up dashboards and allow for more visibility on other error messages.
- The next slide shows and example of dCache billing data from August and September 2023.
- Notes:
 - Requires regular expressions specific to each dataset as trying to do general substitution failed.
 - This is work in progress, only 'completed' for dCache Billing logs and tested in preproduction (but with production datasets).



TOKENIZING - AFTER

• Better visibility of all errors.

• Unique error message count: 124

Top 1000 values of ${\scriptstyle \sim}$	Top 1000 values of error.message.keyword 🗸 🗸 🗸 🗸 🗸 🗸 🗸 🗸 🗸 🗸 ۲ тор 1000 values of error.message.keyword	Count of records \checkmark
10006	Flush was cancelled.	260,899
10006	Stage was cancelled.	104,869
10006	Request to [>CELL_ADDRESS] timed out.	75,804
10006	No redirect from mover on pool PoolName=CELL_NAME PoolAddress=CELL_ADDRESS after 3 min	49,270
10006	Failed to select pool: Request to [>CELL_ADDRESS] timed out.	21,632
10006	No connection from client after 300 seconds. Giving up.	9,768
10006	Transfer killed by door due to failure for mover PoolName=CELL_NAME PoolAddress=CELL_ADDRESS: Request to [>CELL_ADDRESS] timec	189
10006	Request to [>CELL_ADDRESS:CELL_ADDRESS] timed out.	181
10006	Transfer killed by door due to failure for mover PoolName=CELL_NAME PoolAddress=CELL_ADDRESS: (0) Job not found : JOB_ID	55
10006	Failed to deliver message <num:num> to [>CELL_ADDRESS]: CELL_ADDRESS is busy (its estimated response time of NUM ms is longer th</num:num>	31
10006	Failed in state -1: Request to [>CELL_ADDRESS] timed out. [10006]	17
10006	Failed to select pool: Stage was cancelled.	3
10006	Staging timed out	2
10006	Failed to select pool: Staging timed out	1



DCACHE

- Filebeat monitors and ships the contents of dCache's logs.
 - Billing logs contain transaction information within the scope of dCache.
 - Access logs contain transaction information pertaining to the different door protocols (FTP, SRM, WebDAV, XRootD).
- Logstash parses these logs into fields to create Elasticsearch documents, and enrich them as necessary (DNS resolution, GeoIP, tags).
- Packetbeat monitors the door protocol ports to obtain network flows and TLS handshake response times and is aggregated in 1m in and 1h datasets.
- A custom script parses dCache's webadmin pool queue table and sends it to Elasticsearch.





DCACHE OVERVIEW DASHBOARD





TAPE LIBRARY (HSM)

- The library produces SNMP traps when there are failures which are stored in a MariaDB instance from where Grafana queries the information directly.
- Another MariaDB instance that records the tape library's devices and volumes actions.
- A custom script extracts the data and sends it to influxDB where we can manipulate it for later visualization.







TAPE LIBRARY DASHBOARD

~ Overview							
Completed	Bytes Writt	Bu	isiest Drives	Failed Acti	ons by Drive		Total Device Actions. Dev: All
		devname 🐬	actions 🖓	devname 🐬	failures 🐬	10.0 H	DK Total
131.46 к	1.63 тів	<u>changer1</u>	30584	LT08F6C4R3	10514	au 1.01	с 131.5 К С 131.5 К С 105 К
		LTO8F2C3R3	23802	LTO8F6C2R3		ıg Scal	
Eailed Acti	Butos Boad	LTO8F6C4R3	21394			<mark>의</mark> 100.0	0.0
Falled Acti	bytes Redu	LTO8F6C2R3	9116			10.0	
						(00.00 03.00 06.00 09.00 12.00 15.00 18.00 21.00
10.52к	2.26 TiB	Bus	iest Volumes	Failed Actio	ns by Volume		All traps
		volume 🐬	actions 🖓	volume 🐬	failures 🖓	12.5	5 Total
Critical Tra	Warning Tr	<u>S02428L8</u>	22836	<u>S01235L8</u>	10512	10.0	
		<u>S01235L8</u>	21378	<u>S02296L8</u>		Laps	5 WARNING &
Λ	Q	<u>S02081L8</u>	9028	<u>S02081L8</u>		5.0	
-+	\mathbf{O}	<u>S01887L8</u>	8964				
						00	00:00 03:00 06:00 09:00 12:00 15:00 18:00 21:00
				SNMF	P trap description		
Time	Hosts S	♂ Total traps	Severity 🐬 🛛 Trap mes	sage			
2022-11-24 10:42	::30 ts4500-lo	cc1 2	WARNING Trap fo	or drive TapeAlert 0	003. Flag: Hard erro	or. Type:	: W Cause: The drive had an unrecoverable read, write, or positioni
2022-11-24 10:42	::31 ts4500-lo	cc2 2	WARNING Trap fo	or drive TapeAlert 0	003. Flag: Hard erro	or. Type:	: W Cause: The drive had an unrecoverable read, write, or positioni
2022-11-24 10:42	::32 ts4500-lo	c1 1	CRITICAL Trap fo	or drive TapeAlert 0	005. Flag: Read fail	lure. Typ	pe: C Cause: The drive can not determine if an unrecoverable read 1
2022-11-24 10:42	::33 ts4500-lo	cc1 2	CRITICAL Trap fo	or drive TapeAlert 0	005. Flag: Read fail	lure. Typ	pe: C Cause: The drive can not determine if an unrecoverable read 1
2022-11-24 10:42	::33 ts4500-lo	cc2 1	CRITICAL Trap fo	or drive TapeAlert 0	005. Flag: Read fail	lure. Typ	pe: C Cause: The drive can not determine if an unrecoverable read 1
2022-11-24 10:42	::34 ts4500-lo	cc2 2	CRITICAL Trap fo	or drive TapeAlert 0	005. Flag: Read fail	lure. Typ	pe: C Cause: The drive can not determine if an unrecoverable read 1



SYSTEM SYSLOG

- All our hosts' kernel, auth and iptables logs are sent centralized via Syslog to one location and file.
- Filebeat monitors and ships the data.
- Logstash separates the three datasets (auth, iptables, syslog), parsing and enriching as necessary.
- Our goal is to monitor and detect hardware issues, unauthorized logins and network traffic rejections.
- This is one of the datasets we would like to apply machine learning anomaly detection.



LOGINS OVERVIEW DASHBOARD

Interval 10m ~ D	ataSource Tier1 Produ	ction Logs ~												
Accepted - External / 1	Om	Accepted - I	External SSH Login											
		user.name	sou	rce.ip	host.name	system.auth	h.ssh.method	Count						
0.5 0 20:00 00:00 - Successful Total: 1	04:00 08:00 12:00	16:0	-		1									
Failed - Internal / 10m		Failed - Inter	iled - Internal SSH Login											
		user.name		source.ip		host.name		Count						
5						<u>ahw-fe01</u>								
0	01.00 00.00 10.00	10.0				<u>ahw-kvm01</u>								
20:00 00:00 — Failed Total: 18	04:00 08:00 12:00	16:0				ahw-kvm02								
✓ SSH Logins - Exclu Successful SSH Logins	udes 'admin' and 'ba	ckup' Hosts as Sour	ce		Failed Reasons SSH Login Attempts / 10m									
			•	Mean Max Total			Mean M							
20			- Total	0.628 24 91		- 1	— To	tal 39.8 170 5.77 K						
10			— public	key 0.628 24 91	100			ralid 39.8 170 5.77 K						
0			tana da ser		, <u>`~</u> ` ^			ose session: 0						
18:00 21:00	00:00 03:00	06:00 09:00 12	:00 15:00		20:00	00:00 04:00 08:00	12:00 16:0 <mark>—</mark> Fa	n n						
Accepted - Internal SS	H Login				Failed - SSH Logi	in								
user.name	source.ip	host.name	system.auth.ssh.met	Count	user.name	source.ip	host.name	Count						
-	-	gridmon1	publickey	24		2	console	19						
-		gridmon2	publickey	24			console	3						
-		ahw-kvm01	publickey	2			console	2						



LOGINS HOST DASHBOARD





Fernando Fernandez Galindo TRIUMF Scientific Computing Department HEPiX Autumn 2023 Workshop October 16-20, 2023

IPTABLES OVERVIEW DASHBOARD





IPTABLES HOST DASHBOARD

DataSource	Tier1 Production Logs ~ GroupBy sc	ource.as.organizati	on.name ~ H	ostName	ahw-fe01	 Filters 	+ Interval 10n	n ~					
~ NetFilter M	Metrics - ahw-fe01												
Total Rejection	3 K 00:00 06:00 12:00	18:00	Unique Sources	K	50 00:00	06:00 12:	00 18:00	Unique dPorts	3 к	50 25 00:00 06:00	12:00 18:00		
dev		Rejections	Organization	I	P		Rejections ↓	Р	ort		Rejection	s↓	
net0		7.33 K	Tamatiya EOOD	7	9.124.56.254	4	108		23			1.11 K	
			BtHoster LTD		77.90.185.150		93		22	1			
			Chang Way Tec	hn 1	85.81.68.101		70		80			144	
Rejected Pac	ejected Packets by source.as.organization.name				10.183.52.24		66	8,080					
		Valu	CHINATELECON	И Ji 1	17.62.58.82		61	3,389					
	- Chang Way Technologies (Co. Limited 81	Korea Telecom		21.166.2.253		61	4	43			63	
Rejected Packets by source.as.organization.na - Chang Way Tech - DIGITALOCEAN - GOOGLE-CLOU - BtHoster LTD - Chinapet		69	Chinanot	1	112 116 48 122		52	445					
		RM 61			113.110.40.122		52	445					
	Chinanet	/1	CHINA UNICOM	I C 1	124.94.197.168		50	81					
Rejected Pac	kets by source.as.organization.n	@timestamp ▽	id 🗢	dev 🗢	qiso ≙	dOBC ⇔	dIÞ ⇔	db0b. ≙	sISO 🗢	sorg ⊽	sIP 🗢	sPO	
100		2023-10-11 23:16	5:43 ItYHI	net0	CA	Tier-1_SFU		22	CN	Zhengzhou Fasti	42.51.227.67	53	
-:		2023-10-11 23:16	5:41 8HEH	net0	CA	- Tier-1_SFU		50166	US	Tencent Building,	43.130.10.173	60	
10		2023-10-11 23:16	5:38 3tYHI	net0	CA	Tier-1_SFU		11409	GB	GOOGLE-CLOUD	35.203.210.94	55	
		2023-10-11 23:16	8:16 4NYG net(CA	Tier-1_SFU	30000	23	CN	Chinanet	110.183.52.24	47	
1 00:00 04	4:00 08:00 12:00 16:00 20:00	2023-10-11 23:16	6:16 4dYG	net0	CA	Tier-1_SFU	-	23	CN	Chinanet	110.183.52.24	47	
- Chang Wa	y Technologies Co. Limited	2023-10-11 23:16	6:12 ynEGI	net0	CA Tie <u>r-1_</u> SF		-	19885	US	GOOGLE-CLOUD	162.216.149.199	54	
		2023-10-11 23:16	5:12 y3EG	net0	CA	Tier-1_SFU		23	CN	Chinanet	110.183.52.24	47	



HTCONDOR

- Two custom python scripts query the HTCondor:
 - Every 15 minutes to obtain current jobs status.
 - Every 1 hour to obtain job history.
- Both write all information to two different logfiles.
- Filebeat monitors and ships the data.
- Logstash parses these logs into fields to create Elasticsearch documents.





HTCONDOR JOBS' STATUS



Fernando Fernandez Galindo TRIUMF Scientific Computing Department HEPiX Autumn 2023 Workshop October 16-20, 2023

WORKER NODES INLET TEMPS

- A custom script queries all worker nodes' iDrac interfaces to obtain current temperature.
- It writes all information to a logfiles.
- Filebeat monitors and ships the data.
- Logstash parses these logs into fields to create Elasticsearch documents, enriching it with infrastructure data.

0	

WORKER NODES INLET TEMPS

~ Overview

									Ma	ax Devic	e Inlet T	emperat	ure Hist	ory - Per	Rack / 1	1h ~								
2	29	28	28	29	29	29	28	28	28	28	29	29	29	29	28	29	28	29	29	29	28	29	29	29
6	26	25	25	25	25	25	25	25	26	25	25	26	25	25	25	25	26	26	26	26	26	26	26	26
7	29	28	28	28	29	29	28	29	28	28	28	28	28	29	29	29	29	29	29	29	29	29	29	29
8	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28
	22:00	23:00	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00
										,	Average	Inlet Ter	mperatu	re / 10m										
	.				••					•											Ме	an Las	t* Max	c Min
28 °C		-																- wns009	90-drac.de	evices.t1	28.1	°C 29	°C 29°0	; 28 °C
26.00		•••••																wns00	92-drac.de	evices.t1	28.1	°C 29	°C 29°0	28 °C
26 0																	_	wns00	39-drac.de	evices.t1	28.1	°C 29	°C 29°0	28 °C
24 °C	;																	wns009	91-drac.de	evices.t1	28.1	°C 29	°C 29°0	28 °C
22.00																		wns00	13-drac.de	evices.t1	28	°C 28	°C 29°(; 27 °C
22 U																	-	wns00	15-drac.de	evices.t1	28.0	°C 28	°C 29°(27 °C
	22:00	00:	00	02:00	04:00	06:	:00	08:00	10:00	12:	:00	14:00	16:00	18	:00	20:00			1 C - 1		00.0	**		

_____ when 0016 dree devices +1

rage Max Temperature for i...

CURRENT AND FUTURE WORK

- Cleanup of existing datasets and re-processing in some instances.
- Creating 'events' database for overlay on Grafana and classification.
- Creating of time aggregated datasets (e.g. 1hour bins) to both reduce storage usage and normalization.
- Creating Grafana alerts from existing dashboards.
- "Tokenizing" more datasets.
- Creating tools for testing and implementing machine learning tools like anomaly detection, classification, correlation, prediction.
- Identification of datasets that can be brought together to create "vectors" for correlation analysis.
- Investigate the use of GPUs for this type of work.

∂TRIUMF

Thank you Merci

www.triumf.ca

Follow us **@TRIUMFLab**

31

ADDITIONAL MATERIAL

Fernando Fernandez Galindo TRIUMF Scientific Computing Department HEPiX Autumn 2023 Workshop October 16-20, 2023

Python package/module for obtaining/sending data to/from given databases using custom "Request" objects and processing it with a desired tool via "processors".

AFW CONFIG FILE EXAMPLE

Request objects configured via JSON files. Can pass configuration arguments and database queries. Example:

{
 "red
 "nodes": [
 {
 {
 "src": {
 "name": "src",
 "type": "elasticsearch",
 "url": "<u>http://localhost:9200</u>"
 }
 },
 {
 "dst": { ... }
 }
],
]

```
"requests": [
    {
        "name": "src",
        "node": "src",
        "args": {...},
        "body": {
            "query": { ... },
        }
    },
    {
        "name": "dst",
        ...
    }
}
```


CORE ROUTER SFLOW

- Telegraf receives sflow data from our Juniper core router. Only a percentage sample of all data is captured due to its large magnitude.
- Data is stored on influxDB.
- One idea is to implement Snort/Suricata as an intrusion detection system.
- Logs would be sent to Elasticsearch

CORE ROUTER SFLOW

Interval 10m - DataSource	Tier1 Production Logs ~ Group By	destination.address ~ Action	All ~			
Accepted Connect Denied	Connections All - destination.	address / 10m				
• • • •				— Total	Mear	n Total
0	2813 200				42.2	2 6.12 K
•	150				8.49	9 1.23 K
	150	AL AN AMALA		-	5.94	4 861
Unique Destinatio Unique	Source IP's 100				2.33	3 338
					1.93	7 286
\mathbf{a}	50	, • • • • • • • • • • • • • • • • • • •	at a second and the states at a second as a s	-	1.80	6 269
					1.8	5 268
	■ 0 - ***********************************	00 00:00 02:00 04:00 06:0	0 08:00 10:00 12:00 14:00) 16:00 18:00	1.8	3 265
All - Top 10 Destination IP's		All - Top 10 Source IP's		All - Top 10 Protocols		
network.router.juniper.destinatio	Count	network.router.juniper.source.ip	Count	network.router.juniper.protocol		Count
ff02::d	6123	fe80::7a19:f703:903a:7b41	9202	pim		6123
_	849	fddd:7d33:c9b4:ff::22	780	icmpv6		5552
	580	fddd:7d33:c9b4:ff::26	649	icmp		1138
	571	10.0.0.2	578			
	567	fe80::e65d:3700:1b:6774	391			
ff02::1:ffef:f5a	338	172.31.255.44	287			

~ Dynamic Plots (Select aggregation by "Group By" variable)

DCACHE PROTOCOLS (PACKETBEAT)

Packetbeat Flow - Event Count and Duration Percentiles by Protocol - Plots

Packetbeat Flow - Event Count and Duration Percentiles by Host - Plots

2

Fernando Fernandez Galindo TRIUMF Scientific Computing Department HEPiX Autumn 2023 Workshop October 16-20, 2023

SYSTEM SYSLOG HDD ERRORS

Interval auto ~ DataSource Tier1 Production Logs ~ HostName All ~ Filters +									
WNs With SSI	D Error Messages		Events per Host / 1d						
host.name	process.module	Count	100		Distinct Cou	unt Total			
wn334	sd	32		•	— wn334 sda	2 40			
wn334	blk_update_request	8	10 1 0 • • • • • • • • • • • • • • • • • • •	09/18 09/21 09/24 09/27 09/30 10/03 10/06 10/09					
WNs Block Kernel Error Messages									
host.name	process.module	device.name		message.keyword		Count			
wn334	blk_update_request	sda		critical medium error		8			
WNs SD Kernel Error Messages									
host.name	device.name			message.keyword		Count			
wn334	sda			Sense Key : Medium Error [current]		8			
wn334	sda			Add. Sense: Unrecovered read error		8			
wn334	sda			FAILED Result: hostbyte=DID_OK driverbyte=DRIVER_SENSE cmd_age=0s					
wn334	sda			FAILED Result: hostbyte=DID_OK driverbyte=DRIVER_SENSE cmd_age=1s		2			
wn334	sda			CDB: Read(10) 28 00 0f 1d d3 d8 00 00 08 00		2			
wn334	sda			FAILED Result: hostbyte=DID_OK driverbyte=DRIVER_SENSE cmd_age=2s					
wn334	sda			CDB: Read(10) 28 00 0f 1d d5 40 00 00 80 00					

