Verwendung von Kibana im Network Architecture (DNA) Center

Inhalt

Einführung Voraussetzungen Anforderungen Hintergrundinformationen Übersicht über die Kibana-Standardwebseite Anwendungsfälle Rufen Sie alle Protokolle ab, die zum Onboarding-Service gehören. Rufen Sie alle Protokolle ab, die die Zeichenfolge "error" enthalten Kombination und Übereinstimmung Ihrer Suche Abrufen aller Protokolle von einem bestimmten Datum Hinzufügen von Feldern zu einer Suche oder Ansicht Suchen Sie gleichzeitig nach Fehlern aus zwei verschiedenen Diensten. Referenz

Einführung

In diesem Dokument wird beschrieben, wie Kibana verwendet wird, um nach bestimmten Nachrichten oder Protokollen der verschiedenen DNA-Center-Dienste zu suchen.

Mitarbeiter: Alexandro Carrasquedo, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

- Ein DNA-Center-Cluster wird ausgeführt.
- Machen Sie sich mit den Namen und der Verwendung von DNA-Center-Diensten vertraut.

Hintergrundinformationen

Kibana ist ein Open-Source-Datenvisualisierungs-Plugin für Elasticsearch. Sie bietet Visualisierungsfunktionen auf der Oberseite der Inhalte, die in einem Elasticsearch-Cluster indiziert sind und im DNA-Center verfügbar sind. Sie haben zwei Möglichkeiten, darauf zuzugreifen:

- https://<DNA Center ip>/kibana
- Systemeinstellungen -> System 360 -> Tools -> Log Exporter

CISCO CENTER DESIG	IN POLICY PROVI	SION ASSURANCE				.€	9 11 9 11	
System 360 Software Upda	ates Settings Det	a Platform Users Ba	ckup & Restore					
Hosts erra	Service Distribution 🧭						Tools	
10.1.1.1	Deployed	10.1.1.3	Deployed	10.1.1.4	Deployed		Service Explorer	
							Monitoring	
SERVICES 40		SERVICES		528MC85			Log Diplorer	
40	- 1	30	_	43	_		Wakflaw	ł
								1.2

Übersicht über die Kibana-Standardwebseite

Kibana verfügt über mehrere Standardfelder, die in der folgenden Abbildung hervorgehoben sind:

	1.11	85,317 hits					New	Save Open	Share	< O Last	15 minutes 💙
	KIDana	Search (e.g. status:200 AND ext	ension:PHP)						Uses	lucene query	syntax Q
Ø	Discover	Add a filter +									
Ш		logstash-*	0		July 18th 2018, 13:09:10.118	- July 18th 2018, 13:24:10.118 — Auto	•				
\odot		Selected Fields	25,000								0
8		t kubernetes.labels.serviceNa	20,000 - 텉 15,000 -								
۶			0 10,000								
٥		t log	5,000								
		Available Fields	• •	:10:00 13:11:00 13:12:00 13:13:	00 13:14:00 13:15:00	13:16:00 13:17:00 13:18:00 13:19:00 @timestamp per 30 seconds	13:20:00	13:21:00	13:22:00	13:23:00	13:24:00
		 @timestamp 	Time	log				kubernete	s.labels.sen	viceName	level
		t_id	 July 18th 2018 	, 13:24:04.000 [httpd] 172.16.5.20 HTTP/1.0" 204 0 "-"	3 - root [18/Jul/2018:18:24:0 "Jetty/9.2.z-SNAPSHOT" c0131	4 +0000] "POST /write?db=k8s&p=%SBREDAG 330-8ab7-11e8-b212-0000000000000 2866	TED%5D&u=root	influxdb			-
		r Tunney									

- Zeit Zeit, zu der die Nachricht angezeigt wurde.
- Protokoll: Roher Inhalt des Protokolls.
- Kubernetes.label.serviceName Service, der das spezifische Protokoll anzeigt.
- Level Dringlichkeit des jeweiligen Protokolls.

Sie können diese Felder verwenden, um eine umfassende Ausgabe bereitzustellen, die Ihnen bei der Diagnose von Problemen innerhalb Ihres DNA-Center-Clusters helfen kann. Nachfolgend finden Sie einige Anwendungsbeispiele, die Ihnen bei den ersten Schritten mit Kibana helfen.

Hinweis: Dieses Dokument enthält Beispiele für bestimmte Services. Sie können diese Suchvorgänge jedoch nach Diensten ausprobieren, die Ihren Fehlerbehebungsanforderungen entsprechen.

Anwendungsfälle

Rufen Sie alle Protokolle ab, die zum Onboarding-Service gehören.



Rufen Sie alle Protokolle ab, die die Zeichenfolge "error" enthalten

Tipp: Die gängigsten Protokolleinträge, die auf Probleme hinweisen, enthalten "Fehler", "Fehler" und "Ausnahme". Sie können die Zeichenfolge beliebig ändern, damit sie eine andere häufig vorkommende Zeichenfolge ist, die Sie bei der Fehlerbehebung unterstützen kann.

109	g:error												
	Liberto	265 hits							New Sa	ve Open Shar	re 🔇 🛛 Last 1	15 minutes	:
	KIDANA	log:error								U	ses lucene query	syntax	۹
Ø	Discover	Add a filter +											
Ш		logstash-*	0		ju	uly 18th 2018, 13:15:54.89	19 - July 18th 2018, 13:30:54.8	199 — Auto 🗘					
\odot		Selected Fields		40								- 1	0
8		t kubernetes.labels.serviceNa		≝ ³⁰									
×		▲ level		ğ 20				Count	6 Desconde lu	6			
۰		t log		10-				etimestamp per so	seconds ju	iy 18th 2018, 13:2	4:30.000		
		Available Fields	•	13:17:00 13:18:00	13:19:00 13:20:00	13:21:00 13:22:00	13:23:00 13:24:00 @timestamp per 30 seconds	13:25:00 13:26:00	13:27:00	13:28:00 1	3:29:00 13:30:0	00	
		⊙ @timestamp		Time -	log					kubernetes.labels	serviceName	level	
		t_id		 July 18th 2018, 13:30:32.000 	E0718 18:30:32.091432 name may not be empty	7 nanny_lib.go:95]	Error while querying a	piserver for resources	resource	-		error	
		# _score		 July 18th 2018, 13:30:22.000 	E0718 18:30:22.091089	7 nanny_lib.go:95]	Error while querying a	piserver for resources	resource			error	
		t _type t asctime		 July 18th 2018, 13:30:17.000 	2018-07-18 18:30:17,793 No SNMPV3 Credentials fo	ERROR schedulerTh	readPool-6 c.c	.p.a.s.impl.InventorySe	erviceImpl	onboarding-serv	rice	-	
		t docker.container_id endOfBatch		 July 18th 2018, 13:30:16.000 	2018-07-18 18:30:16,241 - failed: ReadTimeoutError("	ERROR - Request to s HTTPConnectionPool(h	erver http://etcd.kube- ost="etcd.kube-system.sv	system.svc.cluster.loco vc.cluster.local', port	al:2379 =2379):	glusterfs-serve	r	-	

Kombination und Übereinstimmung Ihrer Suche

Sie können nach Einträgen suchen, die einer Kombination von Zeichenfolgen entsprechen, indem Sie AND (oder &) zwischen den Zeichenfolgen verwenden.

log:error AND kubernetes.labels.serviceName:onboarding-service



Hinweis: Nicht alle Felder können durchsucht werden.

Wenn Sie nur durchsuchbare Felder im Bereich Verfügbare Felder anzeigen möchten, wählen Sie das Zahnradsymbol aus, und passen Sie die Ansicht an. Sie können auch den Suchtyp definieren, den Sie verwenden möchten, z. B. Zeichenfolge, Boolean, Zahl usw.



Abrufen aller Protokolle von einem bestimmten Datum

Sie können Ihren Suchkriterien ein time-Element hinzufügen. Wählen Sie im Feld "Time Range" eine der folgenden Optionen aus:

	Liboro	59,030 hits					New Sa	ve Open	Share	C Auto-refresh	< Ø Last 15 min	utes >
📐 Kibana		Time Range								/	▼	\odot
Ø	Discover	Quick	Today This week	Yesterday Day before vesterday	Last 15 minutes Last 30 minutes	Last 30 days Last 60 days						
		Relative	This month This year	This day last week	Last 1 hour	Last 90 days						
0		Absolute	The day so far	Previous month	Last 12 hours	Last 1 year		/				
			Month to date	Previous year	Last 7 days	Last 5 years						
بر			Year to date									
۰		Search (e.g. status:200 AND extens	ion:PHP)							Uses	lucene query syntax	Q

- Schnell: Seit den letzten X Minuten, Stunden, Tagen oder Wochen.
- **Relativ**: Von den letzten X Minuten, Stunden, Tagen oder Wochen bis zu einem bestimmten Datum.
- Absolut Von einem bestimmten Datum bis zu einem anderen bestimmten Datum.

Hinzufügen von Feldern zu einer Suche oder Ansicht

Sie können der Standardansicht weitere Felder hinzufügen, um weitere Informationen zu Ihren Protokollen zu erhalten. Wählen Sie im Bereich Verfügbare Felder die Option Hinzufügen aus, und wählen Sie die Felder aus, die angezeigt werden sollen. Nachdem Sie Ihre Auswahl gespeichert haben, werden die Felder in der Hauptansicht angezeigt.

	·			
	kibana	kubernetes.host:10.1.1.3	Uses lucene query syntax Q	
Ø	Discover	Add a filter +		
		logstash-*	() July 18th 2018, 13:39:35.636 - July 18th 2018, 13:54:35.636 - Auto 🗘	
	Visualize	Colortod Fields		0
\odot		Selected Fields	2,000	
•		t kubernetes.labels.serviceNa	tuno di la constanza di la const	
×		A level		
•	Management	t log		
		Available Fields	13:40:00 13:41:00 13:42:00 13:43:00 13:45:00 13:45:00 13:46:00 13:47:00 13:48:00 13:49:00 13:51: 0 @timestamp.ner 30 seconds	00 13:52:00 13:53:00 13:54:00
		 @timestamp 	Time log	kuberneter labels renviceName level
		t_id	Inne - ing	influx@
		t _index	"Python-urllib/3.5"	
		# _score	July 18th 2018, 13:54:35.000 [httpd] 172.16.0.135 [18/Jul/2018:18:54:35 +0000] "POST /write?db=k8s&precision=s HTTP/1.0" 204 0	influxdb -
		t _type	"-" "Python-urllib/3.5" 036ec11a-8abc-11e8-aclf-0000000000000 646	
		t agent	July 18th 2018, 13:54:35.000 [httpd] 172.16.3.23 [18/Jul/2018:18:54:35 +0000] "POST /write?db=k8s&precision=s HTTP/1.0" 400 326 "-" "Python-urllib/3.5" 03f815ff-&abc-11e8-ac21-000000000000 1972	- influxdb
		t asctime	July 18th 2018, 13:54:35.000 [httpd] 172.16.5.203 - root [18/Jul/2018:18:54:35 +0000] "POST /write?db=k8s&p=WSBREDACTEDWSD&u=root	influxdb -
		t code	HTTP/1.0" 204 0 "-" "Jetty/9.2.z-SNAPSHOT" 038408de-8abc-11e8-ac20-000000000000 1194	
		t docker.container_id	July 18th 2018, 13:54:34.000 [httpd] 172.16.0.135 [18/Jul/2018:18:54:34 +0000] "POST /write?db=k8s&precision=s HTTP/1.0" 204 0	influxdb -
		③ endOfBatch	"Yython-urlito/3.5" 03322000-800C-1108-0210-000000000000 918	
		t filename	July 18th 2018, 13:54:34.000 2018-07-18T18:54:34.53240000 I NETWORK [conn7050] received client metadata from 127.0.0.1:40884 conn7050: { driver: { name: "nodejs", version: "2.2.35" }, os: { type: "Linux", name: "linux",	mongodb -
		t first_request_line	architecture: "x64", version: "4.4.0-128-generic" }, platform: "Node.js v6.9.2, LE, mongodb-core: 2.1.19" }	
		t funcName	July 18th 2018, 13:54:34.000 2018-07-18T18:54:34.541+0000 I - [conn7050] end connection 127.0.0.1:40884 (431 connections now	w mongodb -
		t host	dd open)	
	,	kubernetes.host:10.1.1.3		Uses lucene query syntax Q
	kibana	Arid a filter +		
		least the	9	
	Discover	logstash-*	July 18th 2016, 13:39:35.636 - July 18th 2018, 13:54:35.636 - Auto 🗘	
		Selected Fields		0
\odot		t host	2,000	
•		t kubernetes.labels.serviceNa,	8 1,000 -	
بر	Dev Tools	▲ level		
		t log	0	:00 13:52:00 13:53:00 13:4:00
*	management		© @timestamp per 30 seconds	×
		Available Fields	Time - log kubernet	es.labels.serviceName ^ x « » level host
		 @timestamp 	July 18th 2018, 13:54:35.000 172.16.3.37 - [18/Jul/2018:18:54:35 +0000] "POST /write?db=k8s&precision=s HTTP/1.1" 204 influxdb 0 "." "bubon_uplikb(2 5")	
		t_id	e - Python-urtito/3.5	

Suchen Sie gleichzeitig nach Fehlern aus zwei verschiedenen Diensten.

Fügen Sie bei Ihren Suchkriterien mindestens zwei Services hinzu. Stellen Sie sicher, dass die Dienstnamen in Klammern eingegeben sind, und trennen Sie sie durch **OR**.

kubernetes.labels.serviceName:telemetry-agent)



Referenz

- Elastische Suchoptionen
- Apache Lucene Syntax des Abfrageparsers