& cloudaware

Conflux

Description

Conflux is an LMaaS (Log Management as a Service) module offered as part of the Cloudaware platform. Conflux discovers, enhances and aggregates logs from cloud providers such as AWS, Azure and GCP. Besides standard log management functionality such as search and visualization, Conflux provides enhanced capabilities including security, monitoring, alerting, reporting, anomaly detection and forecasting.

Key Features

- Automatically discovers new logging data sources
- Decorates event data with CMDB data such as tags
- Secure API to endpoints for customers to feed custom logs, e.g. application logs, machine syslogs, etc
- Provides complete visibility across all infrastructure tiers:
 - Cloud, e.g. CloudTrail
 - Network, e.g. VPC Flow Logs
 - Operating System, e.g. Syslog
- Analyzes network logs to discover relationships
- Leverages Machine Learning to detect anomalies and perform forecasting
- Long term data retention (up to 7 years)

Competitors and Key Differentiators

- Conflux competes primarily with products like:
 - Sumo Logic
 - o Splunk
 - Graylog
 - Loggly
- Key Differentiators:
 - Discovers new log sources, such as buckets and API endpoints, automatically without depending on human input
 - Decorates event data with cloud provider tags
 - Automatically archives older data into less expensive storage, resulting in a lower cost of ownership
 - Uses Open Standard "Lucene" and "Elasticsearch" query languages
 - Advanced capabilities, such as anomaly detection and forecasting without extra cost

Automatic Log Discovery

Whenever a user creates new objects – e.g. AWS Load Balancers, S3 Buckets and RDS Databases – the cloud provider requests the user to provide a destination logging location, like a bucket or BigQuery table. This flexibility is great, but large cloud consumers end up with hundreds of locations for log storage. This often results in fragmented data.

Traditional vendors, like Splunk and Sumo, rely on customers to configure "push" pipelines. However, as the number of cloud services and application components that generate logging data increases, they often have missing or incomplete data. Another key problem with the traditional "push" approach is that it requires manual action. See step 1.

& cloudaware



Conflux takes a different approach. Instead of relying on users to manually push logs into a log management solution, it relies on CMDB to discover log sources and notify Conflux.



cloudaware.com info@cloudaware.com

+1 (888) 997 3550

1350 Avenue of the Americas, 2nd Floor, New York, NY 10019 This approach based on automated discovery eliminates the need for manual configurations and reduces the possibility of missing log data.

Graph API and Automated Relationship Detection

Conflux analyzes network, spending and security logs to identify relationships and dependencies between objects in CMDB. Using Graph API, users can perform an in-depth impact analysis necessary in security, availability and disaster recovery use cases.



Anomaly Detection

Conflux offers three types of anomaly detection for all of its data:

- Single Metrics detect anomalies in single time series, e.g. Total Spending By Day
- Multi-Metrics detect anomalies across multiple time series, e.g. CPU
- Network Traffic by Instance and Population detect activity that is unusual compared to the behavior of the population, e.g. console users' logins.

Spinburger Automycinal Spinburger																	
under diversity open aligned ali	Top Influencers	A	Anomaly timeline														
1 1	userIdentity.arn.keyword		Overa	ill in the second se													
Image: Subscription of the state of the	arn:aws:sts::447434275168:assume 97	761		2019-	-05-07 00:00		2019-05	-08 00:00	20	019-05-09 00:00		2019-05-10 00:00	2019-05-11 00:00	2019-05-	12 00:00	2019-05-13 00	0:00
Ausurable	arn:aws:sts::191457664785:assume 96	970	View by: eventName.key	word 👻 Li	imit: 10	▼ (So	rted by ma	ix anomaly sco	ore)								
Image: 1 Image: 1 <th< th=""><th>arn:aws:sts::447434275168:assume</th><th></th><th>AssumeRol</th><th>le</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></th<>	arn:aws:sts::447434275168:assume		AssumeRol	le													
amage: 1945/54/075.sume amage: 1945/54/075.sume ber: ber: dot stance Hall GetTop(Attributes amage: 1945/54/075.sume ber: ber: dot stance Hall GetTop(Attributes ber: dot stance Hall	96	702	GetBucketReplicatio	n													
a b	arn:aws:sts::191457664785:assume		GetTopicAttribute	25													
	86 arn:aws:sts::415433800538:assume	954	DescribeInstanceHealt	h													
array array <th< th=""><th>81</th><th>81</th><th>DescribeInstance</th><th>25</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></th<>	81	81	DescribeInstance	25													
And and water Describe/volume Describe/vol	arn:aws:sts::415433800538:assume		DescribeInstanceStatu	IS													
- - 72 0 Describe/LutoScalingGrow 0 Describe/LutoScalingGrow 0	arn:aws:sts::415433800538:assume	/5	DescribeVolume	25													
$ \begin{array}{c} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 $	72	72	DescribeAutoScalingGro														
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	arn:aws:sts::191457664785:assume		DescribeAccountAttribute	25													
Intra-2 1/2 2/19-05-07 0000 2/19-05-09 0000 2/019-05-10 0000 2/19-05-10 0000 <th>72</th> <th>12</th> <th>ListTagsForResourc</th> <th>:e</th> <th></th>	72	12	ListTagsForResourc	:e													
ansakes:191457664785assume 5 Anomalies Servity threshold Interval eventName.keyword Auto Source		363		2019-	-05-07 00:00		2019-05	5-08 00:00	20	019-05-09 00:00		2019-05-10 00:00	2019-05-11 00:00	2019-05-	12 00:00	2019-05-13 00	0:00
56 67 Pering interval Interval Severity tireshold Severity tireshold Interval Severity tireshold Auto Severity tireshold Interval AssumeRole 1me max severity 1-/2 detector found for Influenced by actual typical description job 10 actions GetTopicAttributes 94 927 0 May 9th 2019 97 Count over eventName.keyword GetEducketReplication 94 927 0 May 9th 2019 96 Count over eventName.keyword GetEducketReplication 5094 120.5 6 it higher th5 6 it higher DescribeInstanceHealth 82 May 9th 2019 96 Count over eventName.keyword GetTopicAttributes 5094 120.5 6 its higher th5 6 its isserifieducation DescribeInstanceHealth 1036 May 9th 2019 88 Count over eventName.keyword GetTopicAttributes 2944 120.5 23x higher ht5 6 its isserifieducation Describe/Name_Groups 1036 May 9th 2019 88 Count over eventName.keyword GetTopicAttributes isserifieducatore 2944 <th>arn:aws:sts::191457664785:assume</th> <th></th> <th>Anomalies</th> <th></th>	arn:aws:sts::191457664785:assume		Anomalies														
verning Lato AssumeRice ime max severity dector found for fullence by ortal pical	56	437 S	everity threshold	Interval													
out Not Not Assumation image Not Not Not Not Not Not Not <th< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></th<>																	
Assume®de time max severity 4 detector fund (exclored) actual point description go in point point actual GeldbucketReplication 9 9775 3 May 90 2019 9.97 Count over eventName.keyword Asume8ole eventName.keyword 7755 12.65 3.93 higher th5 th5 3.93 higher th5 3.93 higher th5 3.93 higher th5 3.93 higher th5 th5 1.93 higher th5 3.93 higher th5 th5 th5 1.93 higher th5			warning V	Auto		~											
1 1	eventName.keyword		• warning ~	Auto		~											
94 5027 May 9bt 2019 96 count over eventName.keyword cetBuckeReplication 5094 129.5 3 3k higher th 5 © 0 627 1385 Vag 9bt 2019 83 Count over eventName.keyword cetBuckeReplication 5094 129.5 3 3k higher th 5 © 0 627 1385 Vag 9bt 2019 83 Count over eventName.keyword GetTopicAttributes Count over eventName.keyword GetTopicAttributes Count over eventName.keyword GetTopicAttributes 129.5 * 23 k higher th 5 © 0 5056 1085 Count over eventName.keyword GetTopicAttributes 2044 129.5 * 23 k higher th 5 © 0 5056 05 05 100 1	eventName.keyword AssumeRole		• warning \checkmark time	Auto max severity	/↓ 6	~ etector		found for		influenced by	y .	actual	typical	description	job ID	action	15
eventName.keyword: DescribeInstanceHealth 2 138 0 escribeInstanceStatus 77 3 10 2 2 138 7 2 138 7 2 138 7 2 138 7 2 2 138 7 2 2 138 7 2 2 2 138 7 2 2 2 138 7 2 2 2 138 7 2 2 2 1 2 5 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	eventName.keyword AssumeRole 96 GetBucketReplication	7875	• warning \checkmark time > May 9th 2019	Auto max severity 97	/↓ c e	ventNam	e.keyword	found for AssumeRole	e	influenced by eventName.ke AssumeRole	y eyword:	actual 7755	typical 126.5	description 	job ID th5	action ©	15
82 1985 198 inderdenting ann.agw ord:	eventName.keyword AssumeRole GetBucketReplication 94 GetTopicAttributes	7875	 warning time May 9th 2019 May 9th 2019 	Auto max severity • 97 • 96	/↓ d 6 6	ventNam ount over ount over	e.keyword e.keyword	found for AssumeRole GetBucketR	e Replicatior	influenced by eventName.ke AssumeRole eventName.ke GetBucketRep	y eyword: eyword: blication	actual 7755 5094	typical 126.5 129.5	description ^ 61x higher 39x higher	job ID th5 th5	action ම ම	15
DescribeInstances May 9b 2019 83 count over eventName.keyword GetTopicAttributes 5168.sssumed- 102 NoveRelicinfastr 129.5 23x higher th5 © DescribeInstanceStatus Describe/outmet 7 92.8 7 92.8 129.5 23x higher th5 65 5	eventName.keyword AssumeRole 96 GetBucketReplication 94 GetTopicAttributes 83 DescribeInstanceHealth	7875 5827 1043	warning time May 9th 2019 May 9th 2019	Auto max severity • 97 • 96	/ √ 6 6 6	letector ount over ventNam ount over ventNam	e.keyword e.keyword	found for AssumeRole GetBucketR	e Replicatior	influenced by eventName.ke AssumeRole eventName.ke GetBucketRep eventName.ke GetTopicAttrib	y eyword: blication eyword: butes	actual 7755 5094	typical 126.5 129.5	description [^] 61x higher [^] 39x higher	job ID th5 th5	action ම ම	15
Describe/name/status role/NewRelicin/fast role/NewR	eventName.keyword AssumeRole 64BucketReplication 94 64CTopicAttributes 83 DescribelinstanceHealth 82	7875 5827 1043 1385	warning time May 9th 2019 May 9th 2019	Auto max severity 97 96	/↓ c c c c c	ventNam	e.keyword e.keyword	found for AssumeRole GetBucketR	e Replicatior	influenced by eventName.ke AssumeRole eventName.ke GetBucketRep eventName.ke GetTopicAttrit userIdentity.ai ord:	y eyword: blication eyword: butes irn.keyw	actual 7755 5094	typical 126.5 129.5	description [^] 61x higher [^] 39x higher	job ID th5 th5	action ම ම	15
75 928 outroe Describe/olumes intrgations/newrelic- intrgations/	eventName.keyword AssumeRole 96 GetBucketReplication 94 GetTopicAttributes 83 DescribelnstanceHealth 82 Describelnstances 77	7875 - 5827 - 1043 - 1385 - 361	 warning ~ time May 9th 2019 May 9th 2019 May 9th 2019 	Auto max severity • 97 • 96		ventNam	e.keyword e.keyword e.keyword	found for AssumeRole GetBucketR	e Replication	influenced by eventName.ke AssumeRole eventName.ke GetBucketRep eventName.ke GetTopicAttrib userIdentity.ai ord: arn:aws:sts:44	y eyword: eyword: blication eyword: butes urn.keyw 4743427 d-	actual 7755 5094 2944	typical 126.5 129.5 129.5	description [†] 61x higher [†] 39x higher [†] 23x higher	job ID th5 th5 th5	action ® ®	15
Describe/olume 65 95 eertName.keyword: 0 65 95 Describe/olume.keyword:	eventName.keyword AssumeRole 96 GetBucketReplication 94 GetTopicAttributes 83 DescribeinstanceHealth 82 Describeinstances 77 Toscribeinstances	7875	 warning time May 9th 2019 May 9th 2019 May 9th 2019 	Auto max severity • 97 • 96		ventNam	e.keyword e.keyword e.keyword	found for AssumeRole GetBucketR GetTopicAtt	e Replication tributes	influenced by eventName.ke AssumeRole eventName.ke GetRucketRep eventName.ke GetTopicAttri,it useridentity.a ord: arn.aws.sts:24 5168:assumec role/NewRelic	y eyword: eyword: olication eyword: butes urn.keyw 4743427 d- clnfrastr	actual 7755 5094 2944	typical 126.5 129.5	description [†] 61x higher [†] 39x higher [†] 23x higher	job ID th5 th5 th5	action ® ®	15
bit control control <thcontrol< th=""> <thcontrol< th=""> <thcontr< th=""><th>eventName.keyword AssumeRole 96 GetBucketReplication 94 GetTopicAttributes 83 DescribeinstanceHealth 82 DescribeinstanceS 77 DescribeinstanceSatta 75</th><th>7875 - 5827 - 1043 - 1385 361 928</th><th> warning ~ time May 9th 2019 May 9th 2019 May 9th 2019 </th><th>Auto max severity • 97 • 96</th><th>y ↓ ¢ c c c c c c c c c c c c</th><th>ventNam ount over ventNam ount over ventNam</th><th>e.keyword e.keyword e.keyword</th><th>found for AssumeRole GetBucketR GetTopicAtt</th><th>e Replicatior tributes</th><th>influenced by eventName.ke AssumeRole eventName.ke GetBucketRep eventName.ke GetTopicAttrii userIdentity.a: ord: arn:aws:sts:3-4 5168:assumec role/NewRelici ucture- Integrations/n</th><th>y eyword: eyword: olication eyword: butes irn.keyw 4743427 d- clnfrastr newrelic-</th><th>actual 7755 5094 2944</th><th>typical 126.5 129.5 129.5</th><th>description ⁺ 61x higher ⁺ 39x higher ⁺ 23x higher</th><th>job ID th5 th5 th5</th><th>action ® ®</th><th>15</th></thcontr<></thcontrol<></thcontrol<>	eventName.keyword AssumeRole 96 GetBucketReplication 94 GetTopicAttributes 83 DescribeinstanceHealth 82 DescribeinstanceS 77 DescribeinstanceSatta 75	7875 - 5827 - 1043 - 1385 361 928	 warning ~ time May 9th 2019 May 9th 2019 May 9th 2019 	Auto max severity • 97 • 96	y ↓ ¢ c c c c c c c c c c c c	ventNam ount over ventNam ount over ventNam	e.keyword e.keyword e.keyword	found for AssumeRole GetBucketR GetTopicAtt	e Replicatior tributes	influenced by eventName.ke AssumeRole eventName.ke GetBucketRep eventName.ke GetTopicAttrii userIdentity.a: ord: arn:aws:sts:3-4 5168:assumec role/NewRelici ucture- Integrations/n	y eyword: eyword: olication eyword: butes irn.keyw 4743427 d- clnfrastr newrelic-	actual 7755 5094 2944	typical 126.5 129.5 129.5	description ⁺ 61x higher ⁺ 39x higher ⁺ 23x higher	job ID th5 th5 th5	action ® ®	15
Uperconservations th	eventName.keyword AssumeRole 96 GetBucketReplication 94 GetTopicAttributes 83 DescribeinstanceHealth 82 DescribeinstanceSattus 77 DescribeinstanceSattus 75 DescribeinstanceSattus 75	7875 5827 1043 1385 361 928	 warning ~ time May 9th 2019 May 9th 2019 May 9th 2019 	Auto max severity 97 96 83		ventNam ount over ventNam ount over ventNam	e.keyword e.keyword e.keyword	found for AssumeRole GetBucketR GetTopicAtt	e Replicatior tributes	influenced by eventName.ke AssumeRole eventName.ke GetBucketRep eventName.ke GetTopicAttrii useridentity.ai ord: arn:aws:sts:44 5168:assume role/NewRelici ucture- Integrations/n infrastructure	y eyword: eyword: blication eyword: butes trn.keyw 4743427 d- clnfrastr newrelic-	actual 7755 5094 2944	typical 126.5 129.5 129.5	description ↑ 61x higher ↑ 39x higher ↑ 23x higher	job ID thS thS thS	action © ©	15
DescribeAccountAttributes May 9th 2019 62 count over eventName.keyword DescribeInstanceFeal ord: arr:axes:ts::44743427 2857 129.5 22x higher th5 (a) (b) ListragsForResource 5166assumed- role/WSServiceNoteFic 5166assumed- role/WSServiceNoteFic 5166assumed- role/WSServiceNoteFic 5166assumed- role/WSServiceNoteFic 5166assumed- role/WSServiceNoteFic 5166assumed- role/WSServiceNoteFic 5166assumed- role/WSServiceNoteFic	eventName.keyword AssumeRole 96 GetBucketReplication 94 GetTopicAttributes 83 DescribeInstanceHealth 82 DescribeInstanceStatus 77 DescribeInstanceStatus 75 DescribeVolumes 65	7875	 warning ~ time May 9th 2019 May 9th 2019 May 9th 2019 	 Auto max severity 97 96 83 		etector ount over ventNam ount over ventNam	e.keyword e.keyword e.keyword	found for AssumeRold GetBucketR GetTopicAtt	e Replicatior tributes	influenced by eventName.ke AssumeRole eventName.ke GetBucketRep eventName.ke GetBucketRep eventName.ke GetBucketRep eventName.ke Stesasumec role/NewRelic ucture- infrastructure eventName.ke DescribeInsta	y eyword: eyword: bitcation eyword: butes trn.keyw 4743427 d- clinfrastr newrelic- eyword: eyword: mceHeal	actual 7755 5094 2944	typical 126.5 129.5 129.5	description 61x higher 39x higher 23x higher 	job ID th5 th5 th5	action © ©	15
**i **i eventname.keyword in annawszstsc4a/434// ListTagsForResource 5168:assumed- 72 ron roleWSScveRoleFF	eventName.keyword AssumeRole 96 GetBucketReplication 94 GetTopicAttributes 83 DescribeinstanceHealth 82 DescribeinstanceStatus 75 DescribeinstanceStatus 75 DescribeVolumes 65 DescribeVolumes 65 DescribeVolumes 44	7875 - 5827 - 1043 - 1385 - 361 - 928 - 95 - 326 -	 warning ~ time May 9th 2019 May 9th 2019 May 9th 2019 	Auto max severity 97 96 83		etector ount over ventNam ount over ventNam	e.keyword e.keyword e.keyword	found for AssumeRold GetBucketR GetTopicAtt	e Replicatior tributes	influenced by eventName.ke AssumeRole eventName ke GetBucketRep eventName ke GetTopicAttrit userdentity.a ord: arrawssts:d- 5168.assume infrastructure infrastructure eventName ke Describenstat th	y eyword: eyword: olication eyword: butes irn.keyw 4743427 d- clnfrastr newrelic- eyword: inceHeal	actual 7755 5094 2944	typical 126.5 129.5	description ↑ 61x higher ↑ 39x higher ↑ 23x higher	job ID th5 th5 th5	action ® ®	15
role/AWISServiceRoleF	eventName.keyword AssumeRole 96 GetBucketReplication 94 GetTopicAttributes 83 DescribeinstanceHealth 82 DescribeinstanceStatus 75 DescribeinstanceSt	7875 - 5827 - 1043 - 1385 - 361 - 928 - 95 - 326 -		 Auto max severity 97 96 83 83 		etector ount over ventNam ount over ventNam	e.keyword e.keyword e.keyword	found for AssumeRold GetBucketR GetTopicAtt	e teplication tributes	influenced by eventName.ke AssumeRole eventName.ke GetBucketteg eventName.ke GetTopicAttru ST68assumes Tole/NewRelic ucture- infegrations/n infrastructure eventName.ke Describeinstat th strustertertity.al a ord:	y eyword: eyword: olication eyword: butes irrn.keyw 4743427 d- clinfrastr hewrelic- eyword: egword: inceHeal irrn.keyw	actual 77755 2994 2944	typical 126.5 129.5 129.5	description ↑ 61x higher ↑ 39x higher ↑ 23x higher	job ID th5 th5 th5	action ම ම	15
22 07/10/2010 orAutoScaling/AutoSc aling	eventName.keyword AssumeRole 96 GetBucketReplication 94 GetTopicAttributes 82 DescribeInstanceHealth 82 DescribeInstanceHealth 77 DescribeInstanceStatus 77 DescribeInstanceStatus 75 DescribeInstancetHealth 65 D	7875 - 5827 - 1043 - 1385 361 928 95 - 326 41	warning ~ time . May 9th 2019 . May 9th 2019 . May 9th 2019 . May 9th 2019 .	Auto max severity 97 96 83		etector ount over ventNam ount over ventNam ount over ventNam	e.keyword e.keyword e.keyword e.keyword	found for AssumeRold GetBucketR GetTopicAtt	e Replication tributes	influenced by eventName.kc AssumeRole editors.influence editors.influence editors.influence role/NevRelic curre- ting attractions/in inflastructure eventName.kc Describeinsta th userIdentity.au ord: arnaws.sts:-4.5 5168.assume.	y eyword: eyword: olication eyword: butes irrn.keyw 4743427 d- clinfrastr ewrelic- eeword: inceHeal irrn.keyw 4743427 d-	actual 7755 2944 2857	typical 126.5 129.5 129.5	description ↑ 61x higher ↑ 39x higher ↑ 23x higher	job ID th5 th5 th5 th5	action © ©	15

Auto Discovered Log Sources

Provider	Log
AWS	ALB Access Logs
AWS	AWS Config
AWS	Billing Cost Allocation, DBR and CUR
AWS	CloudFront
AWS	CloudTrail
AWS	ELB Access Logs
AWS	EKS Logs
AWS	RDS Logs
AWS	Route53 Logs
AWS	S3 Access Logs
AWS	VPC Flow Logs
AWS	WAF Logs
GCP	GCP Billing Data
GCP	Google Audit Logs
Azure	Azure Activity Logs
Azure	Azure Billing Data
Azure	Azure Flow Logs
Operating System	Metric Beat
Operating System	File Beat
Operating System	Winlogbeat
Operating System	Packetbeat

Custom Push Via Syslog	Any custom log file
Custom Pull Via Breeze/LogBeat	Any custom log file

Supported Alert Mechanisms

- Email
- Webhook (Generic, PagerDuty, Slack, JIRA, Cloudaware)
- SNS

Reliability and Scalability

Conflux is a highly redundant service with data replicated across multiple cloud providers and regions. Customers can request specific data center locations such as US Only, EU Only, etc.



Security

Granular Access and Audit Controls

Role-based access and audit controls allow you to control and monitor the actions your Conflux users can take, and what data, tools and dashboards they can access.

User Authentication

Conflux supports SAML integration for single sign-on (SSO) via SAML v2 compliant identity providers including Okta, PingFederate, Azure AD, ADFS, CA SiteMinder, OneLogin, Centrify, SecureAuth, IdentityNow, Oracle OpenSSO, Google SAML2 provider and Optimal Id. Conflux can also integrate with other authentication systems, such as LDAP, Active Directory and e-Directory.

Data Encryption In-Transit and At-Rest

Conflux uses industry-standard SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption for data in transit. All forwarders and user sessions are secured in this manner. Electronic messaging is secured by opportunistic TLS encryption on the email gateways.

Conflux encrypts data at rest using Advanced Encryption Standard (AES) 256-bit encryption.

Environment Segmentation

Conflux deployments run in a compartmentalized secure environment, and your data exists on virtually dedicated servers to ensure it remains isolated from other customers' data.