Service Release Notes

November 19, 2020

Manage

This feature will be available on the US1 and US2 deployments soon.

Update - Ingest budgets now have a Scope, replacing Field Value, which defines the log data to apply to a budget. This new budget assignment scheme allows you to have granular control over your ingest budgets while keeping the configuration overhead to a minimum.

November 16, 2020

Apps

New - The AWS Firewall Network app provides visibility into traffic flows, through alerts generated by AWS Network Firewall.

Dashboards

You can now easily link dashboards together to quickly view related data. Each panel can have links to other dashboards. Links have options to include metadata and time range. When viewing the summary tab on a panel with linked dashboards you'll have the option to select from linked dashboards.

November 13, 2020

Search

Update - We're pleased to announce a improved search experience for Data Tier users. You can use the new _dataTier search modifier to restrict a log search to a particular Data Tier (Continuous/Frequent/Infrequent). For more
Security

New - If you have multiple Sumo Logic accounts, we’ve got good news for you: we’ve introduced custom Sumo Logic subdomains. By default, the subdomain in the URL for accessing Sumo Logic is “service”, like this:

`service.sumologic.com`

Multiple orgs with identical domain names can result in authentication headaches. Now, your account owner can replace the “service” subdomain for each of your orgs with a distinct subdomain. For example:

`west1.sumologic.com`

Then, the links that Sumo Logic generates, for example when you share queries or dashboards, will contain your custom subdomain. These subdomain-enabled links will direct the user to the correct account for authentication.

When subdomains are enabled for an org, you’ll see your SAML SP-initiated login options on the Sumo Logic login page.

Apps

New - The Sumo Logic AWS Lambda extension enables you to get instant visibility into the health and performance of your mission-critical applications using AWS Lambda. With this extension and Sumo Logic’s continuous intelligence platform, you can now ensure that all your Lambda functions are running as expected by analyzing function, platform, and extension logs to quickly identify and remediate errors and exceptions.

November 05, 2020

Collection

New - We’re thrilled to announce our new Cloud-to-Cloud Integration Framework.

The Cloud-to-Cloud Integration framework is an extensible system for running fully hosted, pull, and pub-sub based
sources. Traditionally, Sumo Logic collection has been push-based, where we expose an endpoint to which data sources or collector agents push data to us. However, many SaaS applications and Cloud Providers expose event data that describe user, system/application activity which is critical for operations monitoring, security, and compliance use cases. The Cloud-to-Cloud Integration Framework is the system by which we provide integrations to these sources and SaaS applications.

This release comes with two new Sources, Okta and Netskope. Our existing apps are updated to work with these two new Sources.

The Cloud-to-Cloud Integration Framework is an extensible architecture, in which new Sources can be easily added in the future. Check out the Sources we have available in beta.

**Apps**

Update - We’re happy to announce that the updated version of Sumo Logic App for Azure WebApp is compatible with the new Azure Monitor based Collection.

**October 30, 2020**

**Security**

New - We’re pleased to announce a new role capability that allows a Sumo Logic admin to limit the ability of users to create Access Keys. Currently, all Sumo Logic users can create Access Keys on the Preferences page. (Access Keys allow a user to register collectors and to use Sumo Logic APIs.) With the new Create Access Keys capability, you can limit the ability to create Access Keys to only those roles that require it. Note that, with this update, all roles in your Sumo account have the Create Access Keys capability. To restrict access, your Sumo Logic administrator can remove the capability from roles that do not require it.

New - We’ve released a new security policy you can use to set a maximum timeout for Sumo Logic UI web sessions. Sumo Logic users can set their web session timeout on the Preferences page, up to a maximum of 7 days. If you are a Sumo Logic admin with the Manage Organizational Settings role capability, you can now specify the maximum web session timeout period that users in your org can select. For more information, see Set a Maximum Web Session Timeout.
Search

Update - Just wanted to let you know that we've made an underlying change to our XML Parsing library for parsing XML-formatted logs. The following minor behavioral changes will change how results are returned from parsing XML log:

1. Empty nodes will be returned as self closing tags

For example - Consider the following xml log line (see last empty tag)

```
<users><user id="emptytag" role="manager"><first_name>Sally</first_name><last_name>Jones</last_name><email>sally@emailplace.com</email></user><user id="456" role="contributor"><first_name>Bob</first_name><last_name>Smith</last_name><email>bob@emailplace.com</email></user><user></user></users>
```

Query:
```
[sourceCategory=stag/xmltest ("678" or "emptytag")]
| limit 5
| parse xml "/users/user[3]" as first_name nodrop
```

Old lib would return `<user></user>`
New lib would return `<user />`
2. Extra spaces in XML tags will be trimmed.

For example - Consider the following xml log line (see the extra space in yellow)

```xml
<users><user id="678"
role="manager"><first_name>Sally</first_name><last_name>Jones</last_name><email>sally@emailplace.com</email></user><user id="456"
role="contributor"><first_name>Bob</first_name><last_name>Smith</last_name><email>bob@emailplace.com</email></user></users>
```

Query:

```sql
/code/_sourceCategory=stag/xmltest ("678" or "emptytag")
| limit 5
| parse xml "/users/user[2]" as first_name nodrop
```

Old lib would return: 

```xml
<user id="456"
role="contributor"><first_name>Bob</first_name><last_name>Smith</last_name><email>bob@emailplace.com</email></user>
```

New lib would return: 

```xml
<user id="456"
role="contributor"><first_name>Bob</first_name><last_name>Smith</last_name><email>bob@emailplace.com</email></user>
```

October 23, 2020

**Observability**

Update - We have rolled out audit logging support for Monitors. Create, read, update, and delete operations of Monitors are logged in the Audit Event Index.

**Apps**

New - We’re happy to announce the Windows JSON App based on the JSON event log format and provides insight into the operations of the Windows system operation and events so that you can better manage and maintain your environment. The Windows JSON App is based on the JSON Windows event log format and consists of predefined searches and dashboards that provide visibility into your environment for real-time analysis of overall usage of Security Status, System Activity, Updates, User Activity, and Applications.
New - **Active Directory JSON** assists you in monitoring the Windows Active Directory deployment by analyzing Active Directory logs in the JSON based event log format. The app includes predefined searches and dashboards that provide user activity into your environment for real-time analysis of overall usage.

**Manage**

Update - **Webhook payload variables** need to be in mustache format. You do this by wrapping each variable in double curly brackets, like `{{variable}}`. In February 2018 we introduced this format. We did not deprecate the previous
format using a dollar sign, like $variable. Going forward, we will only support mustache format. The US1 and US2 deployments are scheduled to have this update next week.

This change was communicated to administrators of accounts still using the old format. Any existing alerts using the old format have been automatically switched to the new format.

**Metrics**

Change - We made some nice changes to our approach to disabling metric sources that generate too many unique time series. Instead of completely disabling a noisy metric source, we take a more fine-grained approach by dropping the offending dimension or dimensions.

Also, we’ve implemented a global limit for unique time series, across all your metric sources. That gives you some wiggle room—you can have some metric sources that generate lots of unique time series, and as long as the volume across all your metric sources doesn’t exceed the global limit, you’re good. If you are leveraging Short Term retention in Transformation Rules, you also get significantly higher capacity on the cardinality before being impacted.

Finally, we’ve increased the limit of unique time series a Logs-to-Metrics rule can produce. For more information, see [Disabled Metric Sources](#) and [Logs-to-Metrics](#).

**October 20, 2020**

**Search**

New - We’re happy to announce the release of new and improved Lookup Tables. We’ve improved performance, increased the allowable table size, and made Lookup Tables easier to create and manage. You can populate a Lookup Table by uploading a .csv file, using the save operator, or using the new Save to Lookup option when you schedule a search. Lookup Tables are now a first-class content item: you can view and share them from the Sumo Logic Library. To top it off, we’ve provided new versions of the save and lookup operators, plus two brand new operators: lookupContains and cat.

This is the first of many cool updates as we build a new Lookups framework that is intuitive, performant and flexible to support both operational and security analytics use cases.
**Availability** New Lookup Tables are available in all deployments except Sumo Logic's Montreal deployment, pending AWS providing a required AWS service in the Montreal region.

---

**October 19, 2020**

**Manage**

New - [Jira](#) and [Opsgenie](#) webhook connections are now available.

- Opsgenie connections allow you to create incidents based on Sumo Logic alerts within Opsgenie.
- Jira connections allow you to create Jira tickets based on Sumo Logic alerts in Jira Server, Jira Cloud, and Jira Service Desk.

---

**October 8, 2020**

**Apps**

New - We’re pleased to announce the [JMX App](#) that allows you to analyze and gain insights about Java applications in Kubernetes and Non-Kubernetes environment. The dashboards provide a quick glance at various deployment metrics like memory, CPU, GC performance, and thread behavior, so you can troubleshoot unexpected behavior in your Java environment and the applications running in it.

New - The [Nginx ULM App](#) helps you monitor webserver activity in Nginx for both Kubernetes and Non-Kubernetes environment. The preconfigured dashboards provide information about site visitors, including the location of visitors, devices/operating systems, and browsers used; and information about server activity, including bots observed and error information.
New - The **Nginx Ingress ULM App** helps you monitor webserver activity in Nginx Ingress Controller for both Kubernetes and Non-Kubernetes environment. The dashboards provide information about site visitors, including the location of visitors, devices/operating systems, and browsers used; and information about server activity, including bots observed and error information.

New - The **Redis App** monitors the state of the database cluster in Kubernetes and Non-Kubernetes environment. The dashboards provide information about cluster status, resource usage, commands running, and cache hit rate. You can easily determine the health of the cluster by just a glance at the dashboards.
October 6, 2020

Solutions

New - We’re excited to announce the Software Development Optimization solution that helps you to increase release velocity, improve reliability, and comprehensively monitor your software development pipelines with industry-leading metrics and actionable insights generated automatically from development tools such as Jira, GitHub, Jenkins, PagerDuty, Bitbucket, Opsgenie, and more.

October 6, 2020

Observability

Update - The AWS Observability CloudFormation template has been updated to accommodate intuitive naming of individual AWS resources and a new entity inspector that provides more information about the selected entity, and helps you navigate to the corresponding logs or metrics. To update the CloudFormation stack with this new template, please
October 5, 2020

Observability

We’re excited to announce the general availability of our Observability Solution will be rolling out in the next 48 hours! This feature-rich solution expands to new environments like Kubernetes, and includes tools like Transaction Tracing that work together to ensure you are able to efficiently monitor, troubleshoot, and diagnose issues.

Sumo Logic Observability can help you:

- **Monitor** critical indicators of reliability such as errors or latency.
- **Diagnose** or isolate services or resources that might be the immediate cause of reliability issues.
- **Troubleshoot** and uncover root cause(s) to guide recovery as well as on-going application reliability.

As it relates to monitoring, the Observability solution now includes:

- **Unified Alerting**, across logs and metrics data sources with the ability to specify alert criticality, configure detection rules, set up multiple channels for receiving notifications, auto-resolve incidents, and a central landing page to triage, administer and manage alerts.

- **AWS Observability** features 40+ dashboards to monitor infrastructure on AWS in a comprehensive and intuitive manner across AWS accounts, regions and resource types down to individual entities.
Diagnosing incidents just got easier with:

- **Transaction Tracing** to observe apps and microservices to the level of individual requests and pinpoint issues with particular microservices. Our OpenTelemetry standard based tracing capabilities provide an open and flexible standard for observability of microservices transactions without vendor lock-in. If your service package capabilities have been upgraded to include Tracing, you should see a “Tracing” tab available in your Sumo Logic UI. To start using Tracing or taking advantage of our promotion (90 days worth of trial capacity for free), contact your Sumo representative to activate.

- **Re-vamped Metrics Explorer** that decreases the complexity of finding and visualizing your metrics data with a new structured query builder, and an extended range of visualizations for ad-hoc analysis. Mimicking the Dashboard (New) workflow, you now have the same unified experience in the main metrics tab.

- **Global Intelligence for AWS CloudTrail DevOps** that helps on-call staff isolate or eliminate AWS errors (availability, throttling, out of stock) as probable cause for their incidents. Available for Enterprise accounts.

Troubleshooting incidents can now be streamlined thanks to:

- **Root Cause Explorer**, an AIOps breakthrough that helps on-call staff accelerate troubleshooting and root cause isolation for incidents in their apps and microservices running on AWS by detecting anomalies in 500+ AWS CloudWatch metrics and automatically categorizes anomalies by incident timeline, AWS account, region, namespace, entities, AWS tags, and more dimensions. This is not enabled by default in your account, and requires you to install the AWS Observability solution, and be an Enterprise account holder.
Behavior Insights leverages machine learning to detect patterns, outliers, and changes in underlying service behavior to isolate and automatically explain root causes of application issues.

Underneath these capabilities is expanded support for Open Source frameworks including Open Telemetry for tracing data and Telegraf for increasing the breadth of technologies we collect metrics from.

September 30, 2020

Security

Update - We’re pleased to inform you of the availability of additional password policy options as well as the updates to the password forms.

September 14, 2020

Apps

New - We’re pleased to inform you that a new collection process to export metrics from vRops is now available.

September 10, 2020

Manage

New - Participating in Sumo Logic beta programs just got easier. Now, your Account Owner can opt-in to our beta terms and conditions from the Account page in the Sumo UI. You can do the paperwork once, and get access to beta features faster.

September 3, 2020
Apps

Update - Auto-Subscribe AWS Log Groups to a Lambda Function integration is updated with configurable delay and support for filtering log groups using tags.

September 1, 2020

Solutions

New - The AWS Observability Solution simplifies the monitoring and troubleshooting of your AWS cloud infrastructure. Switching across multiple AWS accounts, regions and services to understand service health? Get intuitive views and search capabilities across your AWS hierarchies with our AWS Observability Solution. Get real-time insight in minutes with over 40 out-of-the-box dashboards.

New - Root Cause Explorer is an AWS Observability add-on that helps your on-call staff, DevOps, and infrastructure engineers accelerate troubleshooting and root cause isolation for incidents in their apps and micro services running on AWS. Root Cause Explorer helps you correlate unusual spikes also known as Events of Interest (EOIs) in AWS CloudWatch metrics, using the context associated with the incident.
**Metrics**

New - We are excited to announce the release of the Metrics filter operator. You can use the filter operator to limit the results returned by a metric query. There are several ways you can restrict results whether by aggregation function, or on how many times the value of individual data points meet a value condition over a particular duration.

Update - We’ve updated the Host Metrics Source to improve your metrics query experience. We’ve added a new dimension to the network interface metrics that the source collects: description. So, now you can query network interface metrics by the network interface description.

**Security**

Update - Global Intelligence for AWS CloudTrail is now Global Intelligence for AWS CloudTrail SecOps. You can detect potentially malicious configuration changes in your AWS account by comparing AWS CloudTrail events in your account against a cohort of AWS customers. CloudTrail events are curated from AWS penetration tests and operational best practices. We’ve reduced false positives by filtering out AWS CloudTrail events from legitimate cloud services including AWS itself and CloudHealth by VMware.

---

**August 21, 2020**

**Apps**

New - We’re pleased to announce the Artifactory 7 Logs support in the Artifactory App. You can Install the App by selecting the desired version from dropdown.

---

**August 14, 2020**

**Apps**

New - We’re pleased to announce the etcd3 support in the Kubernetes Control Plane App which provides immediate visibility into etcd3 health, cache statistics, resource usage, and etcd3 logs for quick analysis. On account of metrics renaming in 1.16, the Kubernetes Control Plane App is now available in the below two versions:
August 10, 2020

Manage

New - Health Events are now available to all paid accounts. This includes all Enterprise accounts, and also the Cloud Flex Professional and Cloud Flex Credits Essentials account types. Health events allow you to keep track of the health of your Collectors and Sources. You can use them to find and investigate common errors and warnings that are known to cause collection issues. When used in combination with our Enterprise Audit Apps, Health Events provide a proactive monitoring framework, differentiated from our competitors’ reactive solutions, where you need to debug data collection after having suffered data loss or downtime. At present, Health Events provide observability for Collectors and Sources, however, the framework will be extended to other areas of our service as development continues.
August 7, 2020

Apps

Update - StackRox is updated with security policies to support logical operators. You can now use the AND, OR, and NOT Boolean operators to combine the policy criteria to create highly specific security policies. It also allows you to narrow down the searches to discover the precise image contents, deployment configurations, or runtime activities.

New - We’re pleased to announce the CoreDNS support in the Kubernetes App which provides immediate visibility into CoreDNS health, activity and gives an overview of resource usage within clusters.

August 5, 2020

Collection

New - We’ve a new way to collect CloudWatch Logs using the CloudFormation template which uses the Sumo HTTP Endpoint stored securely in AWS SSM Parameter Store.

August 3, 2020

Metrics

New - We’ve released a new metric operator: outlier. You can use the outlier operator in metric queries to identify and
visualize metrics data points that are outside the range of expected values.

July 31, 2020

Manage

Upcoming - On August 31, 2020, Sumo Logic will end support for Internet Explorer 11. We recommend that you find an alternative browser as soon as possible.

Search

New - Behavior Insights comes with three new log search operators to accelerate insights, troubleshooting, and action plans using structured logs. Behavior Insights helps answer the following questions:

• What activity patterns are evident from structured logs?
• What patterns are trending?
• Which groups of users, apps, services, or resources are responsible for regular and irregular activity in logs?

Modeled after LogReduce, the new operator LogReduce Keys clusters JSON logs based on keys providing an at-a-glance summary of patterns in logs based on their schema while ignoring specific values. The new operator LogReduce Values clusters JSON logs based on the values of keys.

The third Behavior Insights operator, LogExplain, finds the root cause of outliers in logs based on conditions you specify.

July 30, 2020

Collection

New - Archive lets you forward log data from Installed Collectors to AWS S3 buckets to collect at a later time. If you have logs that you don't need to search immediately, you can archive them for later and ingest them on-demand with hourly granularity.

The key new components provided are:

• An AWS Archive Destination that lets you set up your AWS S3 buckets as archive destinations.
• A Processing Rule type, "Archive messages that match" that archives log data with Installed Collector Sources.
• An AWS S3 Archive Source to ingest data from an Archive destination.
• An Archive page to view all the AWS S3 Archive Sources and ingestion jobs in your account, as well as creating ingestion jobs.

![Table Image]

July 23, 2020

Dashboard (New)

New - We’re proud to announce the release of Dashboard (New), which provides you deeper visual control across logs and metrics data-sources, so you can build the perfect dashboard for your monitoring and troubleshooting needs. This is the first of many cool updates as we build towards a dashboard framework that is visually expressive, troubleshooting optimized, and hyper-performant.

![Dashboard Image]

July 14, 2020

Search

Update - Scheduled Searches now have a maximum allowed time range for each frequency. The following are the new maximum time ranges by frequency:

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Max Allowed Time Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Time</td>
<td>15 min</td>
</tr>
<tr>
<td>15 min</td>
<td>1 Day</td>
</tr>
</tbody>
</table>

Copyright 2020 Sumo Logic, Inc. All rights reserved.
### July 10, 2020

**Apps**

Update - The [Cloudflare](https://cloudflare.com) app dashboards have been substantially improved with optimized queries by eliminating unwanted parsing and enhancing the lookup positions through optimization.

### July 7, 2020

**Manage**

New - Read all about our new [Certification and Training](https://sumologic.com/certification) site which you can access from the Certification tab in the product. We've added an Onboarding section as well as improved your self-paced and test-taking experience. Also, Certification exams in Spanish and Japanese are readily available in any production environment so have fun and get Certified!

**Security**

New - Sharing is good, over-sharing, not so much. So, we've added a new security policy you can use to ensure that shared dashboards don't display data that users they're shared with shouldn't see. The new policy is [Data Access Level for Shared Dashboards](https://sumologic.com/help/data-access-level-for-shared-dashboards). If your role grants you the "Manage organization settings" capability, you can enable the new policy on the **Manage > Security > Policies** page. By default, once you enable this policy, any newly-created dashboards will run under the role search filter of the users it is shared with.
Also with the goal of giving you better control of your data, we've introduced a new role capability: "Change Data Access Level of Dashboards". Users with this capability can change the data access level of dashboards that are shared with them with edit or manage permission.

---

**June 25, 2020**

**Search**

Update - An underlying change has occurred in the [ASN lookup](https://example.com) operator because of a change made by our vendor. You may see the organization ID instead of the name in the results. We are working on an update to make things consistent, but for now, you may see unexpected returns.

**Apps**

Update - We have optimized the searches in dashboard panels in the [Akamai CloudFront](https://example.com), [Akamai Cloud Monitor](https://example.com), and [Fastly](https://example.com) app dashboards.

---

**June 18, 2020**

**Metrics**

New - There's a new operator in town: `fillmissing`. This metric operator comes in handy for metric data sets in which some timeslices contain no data points. You can use `fillmissing` in a metric query to fill empty time slices in metric query results with a derived data point. You can choose between several methods of deriving a data point, or leave empty timeslices empty.

---

Copyright 2020 Sumo Logic, Inc. All rights reserved.
Search

Update - The volume of data scanned is displayed on the Search page when searching an Infrequent Tier Partition.

June 16, 2020

Search

New - We are pleased to announce the General Availability of the Search Audit Index which provides event logs on search usage and other activities for your account. The index allows you to monitor and audit the search queries being run within your account, the types of queries, the users running them, and more. This is available only to our customers in Enterprise account types (Enterprise, Enterprise Operations, Enterprise Security, and Enterprise Suite).

Apps

New - We are pleased to announce the General Availability of the Enterprise Search Audit App, which provides immediate visibility into your account's search activity and gives an overview of search usage within your org. The pre-configured dashboards help you identify opportunities for improving search performance using the Search Audit Index. This app is only available for our Enterprise customers (Enterprise, Enterprise Operations, Enterprise Security, and Enterprise Suite).

You can use the Enterprise Search Audit App, only if an administrator has enabled the Search Audit Index. For more information, see Enable and Manage the Search Audit index.
Security

Update - By popular demand, we’ve made some changes to the capabilities you can assign to roles in Sumo Logic. Our goal was to give you more fine-grained control of Sumo functionality when you set up roles. Here’s what we did:

- We replaced the Manage Indexes capability with four new capabilities: View Partitions, Manage Partitions, View Scheduled Views, and Manage Scheduled Views. Any existing role that previously had the Manage Index capability now has the four new capabilities.
- We provided new capabilities that you can use to provide view-only access to Field Extraction Rules.
- We added two capabilities related the Fields feature: View Fields and Manage Fields.

So what do you need to do because of this change? There’s nothing you have to do. However, if you’d like to let users view information about resources like Partitions, Scheduled Views, Fields, and Field Extraction Rules without letting them change them, you can easily accomplish that with the new view-only capabilities.

Search

Update - Scheduled Search no longer permits Static Time ranges to be set when scheduling a search. You must choose a relative time range. This is to ensure the longevity of your scheduled searches and to help you get useful results.
June 5, 2020

Apps

New - We are pleased to announce Global Intelligence for AWS CloudTrail DevOps, which guides infrastructure engineers, on-call staff and DevOps users to accelerate root cause analysis for incidents through error rate and configuration insights benchmarked from our AWS customers for the following AWS services:

- EC2
- Lambda
- Auto Scaling
- S3
- ELB
- RDS
- DynamoDB
- ElastiCache
- Redshift

The benchmarks rely on 15 million data points per week from AWS CloudTrail logs and baseline service availability, throttling, account quota and insufficient capacity/out-of-stock errors in 27 AWS regions by AWS service, API, account, and instance type. The app recommends configuration improvements to key AWS services based on baseline usage such as memory and concurrency settings for AWS Lambda, provisioned IOPS for DynamoDB and min/max sizes of EC2 Auto Scaling groups.
May 21, 2020

**Collection**

New - We have [Extended HTTP Metadata Collection](#) capabilities. HTTP Sources receiving log data can now process headers into metadata fields.

New - Kubernetes Collection 1.0.0 introduces multiple enhancements to the collection process.

- Standardized and reorganized the configuration options in the `values.yaml` for clarity and ease of use.
- Exposed full control of the Fluentd pipeline with `values.yaml` which allows you to easily extend the collection process. You can fork data to multiple destinations, add custom log sources, and attach additional filters to the Fluentd pipeline.
- Reduced the default collected metrics to only what the Kubernetes apps require.
- Split the FluentD Deployment into two StatefulSets, one for logs and one for metrics. This change enables better use of persistent volumes and improved buffering.
- Falco has been disabled with an upgrade to a more recent version which disables the BitCoin mining rule that affected AWS GuardDuty users. We have also disabled Falco by default while we work through the incompatibilities with certain operating systems.

You can read more about the changes in our [migration document](#).

Since this is a breaking change if you're running earlier versions of collection, we have provided a [migration guide and migration script](#) to make it much easier for you to upgrade to this release.

---

May 20, 2020

**Manage**

We've made it easier for you to Manage Logs and Metrics settings by removing the generic Settings area. This should help you easily locate which settings you want to manage for Logs or Metrics:

- Logs: [Fields, Field Extraction Rules (FERs), Partitions, Scheduled Views, Data Forwarding](#)
May 18, 2020

**Security**

New - We added a new role capability you can use to control access to the Account Overview page in Sumo Logic. Previously, any Sumo user had view-only access to this page. The new capability is View Account Overview, and your Account Owner, and users with the Admin role now have it. Your Sumo administrator can assign the capability to other users or roles, as desired. Because users without the capability won't be able to see the Account Overview page, where your Organization ID is shown, we've updated the Preferences page in the Sumo Logic UI to also display your Organization ID. That way, users who can’t view the Account Overview page can find your Organization ID, useful when dealing with Sumo Support.

If you previously had access to the Account Overview page and need the information it contains, contact your Sumo administrator to obtain access.

May 5, 2020

**Collection**

Sumo Logic now supports collection from AWS GovCloud regions. AWS GovCloud is a set of specific regions authorized to a FedRAMP-High baseline. GovCloud regions meet higher regulatory and compliance requirements set by government agencies and U.S. customers that manage sensitive data in the cloud. These regions are where users with strict compliance requirements may operate in adherence with ITAR, FedRAMP, and DoD requirements. Users of Sumo Logic can now collect logs and metrics from AWS services and sources running with GovCloud, assuring that customers can continue to meet their regulatory requirements while using our Operational Intelligence Platform.

While Sumo Logic does provide collection of logs and metrics from GovCloud regions, Sumo Logic does not itself run in AWS GovCloud. Be aware, collection of data from AWS GovCloud means logs, metrics, and data will be leaving a FedRAMP-high environment. For this reason, we recommend that customers with elevated compliance and regulatory requirements use our FedRamp deployment.

April 30, 2020

**Apps**

New - The Infrequent Data Tier App provides visibility into the On-demand Search usage and costs associated with Infrequent Data Tier by providing intuitive pre-configured dashboard and searches. Infrequent Data Tiers are an economical, fully managed log analytics solution for high volume, infrequently accessed data. With Infrequent Data
Tiers, organizations have a solution that can aggregate, store and analyze verbose sources such as App Debug, CDN, Load Balancer, and other infrequently accessed logs at a dramatically lower price point.

Collection

New - Sometimes good things come in threes. That's true of our Data Tiers—we have added the Infrequent tier to keep the Continuous and Frequent tiers company. (Data Tiers are what we previously called Analytics Tiers.)

The Infrequent tier is a cost-effective, fully managed log analytics solution for high volume, infrequently accessed data. This tier allows you aggregate, store, and analyze verbose data that you access infrequently, like debug, CDN, and load balancer logs—at a dramatically lower price point, starting at only 10 cents per GB ingested.

The Infrequent tier is only available only in Enterprise Suite available with Cloud Flex Credits packaging.

April 21, 2020

Search

The Field Extraction Rules page has a new look and shows you the total number of fields your rules are using. When creating a rule you'll see and can select specific fields you want the rule to assign.

April 17, 2020

Integrations

New - VMware AirWatch Integration with Sumo Logic provides visibility for monitoring enterprise mobility management in your deployment. The unified digital workspace platform simplifies and secures app access and IT management throughout your environment. VMware AirWatch is an enterprise mobility management (EMM) software and standalone management systems for content, applications and email.
April 13, 2020

Apps

New - The Zoom App provides visibility into how Zoom is being used across your organization, displaying analytics on performance, availability, security, and user activity. The app aggregates and reports on data so you can correlate and investigate trends and respond to incidents across all of your IT tools in a consistent and timely manner. Zoom uses Webhook events, that are documented in full on this Zoom web page.

Update - The Kubernetes App has two new dashboards:

- The Kubernetes - DPM dashboard provides insights into where Data Points Per Minute (DPMs) originate so you can determine ways to reduce them for optimum performance. Panel analytics show DPMs by collector, namespace, pod, container, and cluster.
- The Kubernetes - DPM Timeseries dashboard provides visibility into the number of DPM timeseries and their breakdowns. This, combined with DPM analytics, enables you to determine ways to reduce DPMs for optimum performance.

March 30, 2020

Solutions

New - The Atlassian Solution integrates all of your Atlassian cloud tools to provide real-time DevOps monitoring and troubleshooting capabilities throughout your environment. By leveraging data from multiple Atlassian products, the Sumo Logic Atlassian solution enables development teams to benchmark their performance in minutes against the industry-
leading metrics and drill down into actionable insights to continuously improve their software delivery performance.

Sumo Logic Apps for the Atlassian products:

- **Jira Cloud** - Provides insights into project management issues to more effectively plan, assign, track, report, and manage work across multiple teams.
- **Jira** (Server) - Provides insights into Jira usage, request activity, issues, security, sprint events, and user events.
- **Bitbucket** - Provides insights into project management to more effectively plan and manage development and deployments.
- **Opsgenie** - Provides at-a-glance views and detailed analytics for alerts on your DevOps environment.
- **Atlassian** - Integrates access to all your Atlassian cloud tools with real-time monitoring capabilities across your environment.

---

**March 27, 2020**

**Security**

New - We’ve added a new Sumo Logic security policy—**Per User Concurrent Sessions Limit**—that you can use to limit the number of sessions users can have open at a time. For increased account security you can implement this new policy to help prevent user account sharing.

Update - If you’re a Sumo Logic administrator, check out our new and improved UI for managing users and roles in Sumo Logic. The new UI provides a more streamlined experience with a side panel for creating and editing users and roles.

---

**March 25, 2020**

**Solutions**

New - The **Work From Home Solution** is a suite of in-depth apps to support businesses transitioning to a remote workforce. This Solution provides visibility and management for your remote workforce with SSO, remote access, endpoint security and productivity SaaS apps to ensure that your employees can work from home productively and...
safely. Monitor availability, performance, user activity and collaboration, and security across your workforce locations.

March 17, 2020

Metrics

Update - The rate metric operator now supports two new options: increasing and decreasing. These options are useful when you are calculating the rate of change of a counter over time. If you use the increasing option, the operator will consider only those pairs of consecutive points where the second point in the pair is greater than the first point. Similarly, if you use the decreasing option, the operator will consider only those pairs of consecutive points where the second point in the pair is less than the first point.

March 10, 2020

Apps

Update - Audit app has added a new Scheduled Search - Triggered Summary dashboard that provides information on scheduled searches that have been triggered, along with details on related alerts and Webhooks.

March 3, 2020

Partner Apps

New - Partner App for Alcide kAudit. The Alcide kAudit app automatically analyzes Kubernetes audit logs to detect anomalous behavior of users and service accounts. kAudit automatically detects security-related issues related to Kubernetes' administrative actions, especially anomalous behavior that can only be detected from observing extended context over multiple activities. In addition, kAudit supports Audit rules to detect violations of organization compliance.
policies regarding Kubernetes usage. Incident forensics, along with audit statistics, are presented in graphical and tabular summaries for easy investigation and analysis.

New - Partner App for ARIA Packet Intelligence app. The ARIA Packet Intelligence app, by ARIA Cybersecurity, creates unsampled NetFlow or IPFIX metadata for every network packet. This allows for the detection of network-borne attacks, including ransomware, malware, APTs and intrusions early in the kill chain before significant harm occurs. It provides visualization and profiling of all internal network traffic, within a Sumo Logic environment, to detect possible threats and verify connectivity policies.

---

March 2, 2020

Metrics

Update - We’ve simplified the configuration options for metric monitors. Previously, the condition for triggering a critical or warning alert was based on a threshold metric value, a time duration, and the percentage of the time duration that metrics were above or below the threshold value. We removed the percentage of time option because we found that customer usage of it was very low.

---

February 13, 2020

Collection

Beta - Collection Health Events allow you to keep track of the health of your Collectors and Sources. You can use them to find and investigate common errors and warnings that are known to cause collection issues. When used in combination with our Enterprise Audit Apps, Health Events provide a proactive monitoring framework, differentiated from our competitors’ reactive solutions, where you need to debug data collection after having suffered data loss or downtime. At present, Health Events provide observability for Collectors and Sources, however it will expand to other areas of our service as development continues. This is available as a closed Beta to Enterprise accounts. To participate contact your Sumo Logic account executive or sign up for an enterprise trial account.

---

February 12, 2020

Search

New - Lookup autonomous system information for an IP address with the ASN Lookup operator.

---

February 10, 2020

Search

Update - Webhook alerts now support sending an alert for each result returned from a scheduled search.
February 7, 2020

**Apps**

**New - Global Intelligence for Amazon GuardDuty**

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. The Sumo Logic App for Global Intelligence for Amazon GuardDuty analyzes GuardDuty threats from the Sumo Logic population to create baselines of threats. These baselines enable you to optimize security posture and remediation based on how unusual your GuardDuty findings are compared to Sumo Logic customers. The App includes pre-configured dashboards and searches with visual displays for global threat baselines and real-time threat detection across your AWS environment.

**New - Global Intelligence for AWS CloudTrail**

The Global Intelligence for AWS CloudTrail App enables you to detect potentially malicious configuration changes in your AWS account by comparing AWS CloudTrail events in your account against a cohort of AWS customers.
CloudTrail events are curated from AWS penetration tests and operational best practices.

January 13, 2020

Connections and Integrations

New - You can now set up a ServiceNow Incident Webhook connection, and create scheduled searches for the connection. Webhook connections allow you to send Sumo Logic alerts to third-party applications that accept incoming Webhooks.