vRealize Log Insight Release Notes

VMware Aria Operations for Logs

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

What's New March 2023

1

- **Azure Sentinel Log Forwarding Support:** You can forward logs from vRealize Log Insight Cloud to Azure Sentinel. Refer documentation for more details.

What's New February 2023

2

- **Tanzu Kubernetes Grid multi-cloud Auditing (Update).** This update includes support for Fluent Bit in addtion to Fluentd. The Tanzu Kubernetes Grid multi-cloud (TKGm) Content Pack is updated to include content for API server logs, controller logs, scheduler logs, pod related logs, and so on, along with alerts for K8 events. Updated dashboard and queries include API Server Overview, Controller Manager Overview, Scheduler Overview, Control Plane Events, Pod Related Events, and Velero Related Events.
- **Search By Log Timestamp**: You can now search logs by Log Timestamp present in the log payload. Refer Searching and Filtering Log Events for more details.

What's New January 2023

3

- **Content Migration**: You can now migrate content such as Dashboards, Queries, Alerts, and Extracted Fields from vRealize Log Insight (on-premise) to vRealize Log Insight Cloud by using vRealize Cloud Connect. For more information, see How to migrate vRealize Log Insight using vRealize Cloud Connect.
- **Extracted Fields with Improved User Experience:** With the revamped User Experience, you can extract fields on the Explore Logs screen without losing the context. Also, the new Fields Library page lets you search and filter the fields in a seamless manner.
- **Multiple Availability Zones:** The vRealize Log Insight Cloud service in a region is now deployed across multiple availability zones (AZs), helping the service handle AZ failures. This multi-AZ support provides high availability in terms of user interface, data ingestion, and log querying when an AZ is not available. **With this release, multi-AZ support is available in all the regions**. You can view the detailed documentation here.
- **Deprecated Feature:** *Variable Retention* is deprecated. Post January, you will not be able to create and edit the existing variable retention configurations. You must migrate your configuration to the new *Log Partitions* feature as this deprecated feature will be removed in upcoming release. Log partitions let you ingest logs and store them based on the policies or rules that you define for each partition. Similar to variable retention, you can specify a retention period for each partition, which is the number of days for which you want to retain the logs.

What's New December 2022

4

- **Content Pack Release**: The following updated content packs are now available with rich set of out-of-the-box content such as queries, dashboards and alerts.
  - **vSAN Content Pack** provides powerful insight into your vSAN logs, letting you make informed and proactive decisions within your environment. This update includes vSphere8.0 release support, vSAN ESA support, and refined disk events category and monitoring
  - **vSphere Content Pack** provides powerful insights into your vCenter Server and ESXi logs, letting you make informed and proactive decisions within your environment. This update includes vSphere 8.0 release support, vSAN ESA content support, new vSAN alarms, and a few critical bug fixes
  - **vCloud Director Content Pack** provides information from vCD that will help you have a complete picture of the health and operational status of your private cloud. This update includes newly added content for vApps Created/Imported, Updates On Queries for vApps, VMs and vCD, and a few critical bug fixes.
  - **NSX-T Content Pack** provides health status dashboards for the logical switching and routing, distributed firewall, and DHCP components that make up the NSX infrastructure. It also provides key audit logs for tracking create, add, and delete changes to your NSX infrastructure. This update includes newly added content for alarms, events, and firewalls. It also includes updates on existing content for password-related events, communication errors, system-related metrics, certificate expiry, and security service.
- **AVS Syslog Enhancements:** Azure VMware Solution (AVS) logs provide powerful insights into the events generated in your AVS SDDC. This syslog update extracts more information that logs contain by parsing the new fields such as time and location and extracting the data from the nested fields, making it easier to query using the fields.

What's New November 2022

5

- **Multiple Availability Zones:** The vRealize Log Insight Cloud service in a region is now deployed across multiple availability zones (AZs), helping the service handle AZ failures. This multi-AZ support will provide high availability in terms of user Interface, data ingestion, and log querying when an AZ is not available. Currently, multi-AZ is available in the US region only. Other regions will soon get the same support. You can view the detailed documentation here.
- **vRealize Log Insight On-Premise integration:** You can integrate vRealize Log Insight on-premise with vRealize Log Insight Cloud without using a Cloud Proxy. This brand new page will give you a centralized view of all your on-premise instances with details such as health status, usage patterns, and more. For detailed documentation, visit this page.
- **SSL Support in Log Forwarding to TCP endpoints:** Securely forward logs from vRealize Log Insight Cloud to your syslog server for TCP endpoints.
- **Pre-Ingestion Filtering (Beta):** You can save ingestion costs for unwanted logs sent to vRealize Log insight Cloud by filtering the data at the source (Cloud Proxy).

What's New October 2022

6

- **REST-based Public API Support**: Automate alerts, queries, and more with vRealize Log insight Cloud through the REST API. You can find the API documentation here. The BETA APIs listed here will be decommissioned in the upcoming releases.
- **Improved Integration with vRealize Operations Cloud**: You can now configure vRealize Log Insight Cloud alert definitions to send log alerts and notifications to vRealize Operations Cloud.
- **vRealize Log Insight On-premise Custom Content support:** You can now export vRealize Log Insight on-premise custom content and import into vRealize Log Insight Cloud as private content. The content may include dashboards, alerts, queries, and extracted fields. You can find the content pack export documentation here.
- **Content Pack Release:** The following new and updated content packs are now available with a rich set of out-of-the-box content such as queries, dashboards and alerts.
  - **Tanzu Kubernetes Grid multi-cloud Auditing (New)** is now available with rich set of out-of-the-box content such as dashboards, queries and extracted field for Kubernetes api server logs, controller logs, and scheduler logs. This helps with consistent, upstream-compatible, regional Kubernetes substrate across software-defined datacenters (SDDC) and public cloud environments.
  - **Cisco UCS content pack (New)** provides insights into the syslogs of UCS Manager, letting you make informed and proactive decisions within your UCS domains.
  - **Linux NIX content pack (Update)** provides information about the key entities of any Linux operating system installation health and ability to monitor file-system logs. vRealize Log Insight Cloud offers a very intuitive graphical representation, especially with regard to log events. This update includes 14 new dashboards around Security Monitoring, System Application Events, Email, and Syslog Information.
  - **vSphere content pack (Update)** provides powerful insights into your vCenter Server and ESXi logs, letting you make informed and proactive decisions within your environment. This update includes quality improvements.

- **Deprecated Features:** *Log Archival* and *Variable Retention* are deprecated with immediate effect. You must migrate your configuration to the new *Log Partitions* feature before these deprecated features are removed. Log partitions let you ingest logs and store them based on the policies or rules that you define for each partition. Similar to variable retention, you can specify a retention period for each partition, which is the number of days for which you want to retain the logs.

What's New August 2022

7

- **Log Root Cause Analysis (RCA):** Log RCA helps you find the potential root cause for major issues from a million log messages. When you trigger an investigation around the incident time window, the log RCA service detects and surfaces relevant logs in the form of log clusters as a potential root cause.
- **Log Compare:** Detect anomalies in log streams across time or across log sources. This helps you determine what was different right before a release or a failure as compared to the previous day or previous week.
- **Log Forwarding in RAW Format over TCP/UDP**: You can now forward logs in RAW format in addition to the existing JSON format.
- **Content Pack Page with Improved User Experience:** Content packs are now grouped based on names for different versions for improved visualization and to provide an easy upgrade experience.
- **Log Sources Page with Improved User Experience:** You can now search for log sources and filter them based on categories such as Agents, Applications, Application Development, Protocols, and many more.
- **Handle Conflicting Fields:** There are certain fields like "id", "timestamp", "log_timestamp", and "_version_" that vRealize Log Insight Cloud uses for internal processing. If such fields are detected during log ingestion, they conflict with the internal fields, resulting in some of the logs being dropped. To prevent this issue, logs with such fields are now appended with "_message_payload" .
- **OCVS Content Pack:** Running natively on Oracle Cloud, the Oracle Cloud VMware Solution (OCVS) vSphere content pack provides powerful insights into your vCenter Server and ESXi logs, letting you make informed and proactive decisions within your environment. The OCVS NSX-T content pack provides health status dashboards for the logical switching and routing, distributed firewall, and DHCP components that make up the NSX infrastructure. It also provides key audit logs for tracking create, add, and delete changes to your NSX infrastructure.
- **AVS Content Pack :** The Azure VMware Solution(AVS) content pack provides powerful insights into private clouds that contain vSphere clusters built from a dedicated bare-metal Azure infrastructure.

- **VMware Cloud Disaster Recovery (VCDR) Log Support**: Forward VCDR event logs to vRealize Log Insight Cloud and analyze event logs related to protection, recoverability, and user interactions. You can forward VCDR logs within a specific time range in the past, from a time starting in the past to the present, from a time in the past going forward, or from the present moving forward.

What's New July 2022

8

- **Service Proxy Resource Customization:** You can modify the CPU and memory resources for a service proxy. Modifying these resources lets you override the default configuration to accommodate higher log ingestion rates. Refer here for more information about modifying resources for a service proxy.
- **Log Forwarding with Ingested Fields**: vRealize Log Insight Cloud lets you forward all or a subset of incoming log events to a syslog or HTTP endpoint. Now, you canalso forward all theingested fields of logs to a Splunk endpoint. To enable this configuration, select the **Forward all fields** check box in your log forwarding configuration.
- **VMware AVS Support:** Logs from Azure VMware Solution (AVS) are now available in vRealize Log Insight Cloud. These logs include vCenter and ESXi Hosts audit logs and NSX-T firewall packet logs to support compliance and troubleshooting use cases.
- **VMware OCVS Support:** Logs from Oracle Cloud VMware Solution (OCVS) are now available in vRealize Log Insight Cloud. These logs include vCenter and ESXi Hosts audit logs and NSX-T firewall packet logs to support compliance and troubleshooting use cases.

What's New June 2022

9

- **Improved Onboarding Experience:** Introducing the Knowledge Hub - a repository of in-product guides that provide step-by-step walkthroughs to configure different features, video, config, and blog resources, and release notes.
- **Improved Contextual Error Messages:** Product pages such as Dashboards, Alerts, Subscriptions, vSphere Integration, Log Forwarding, and others are now improved with contextual error and trace references.
- **vRealize Log Insight On-premise Log Collection:** The vRealize Log Insight on-premise collector runs as a part of the vRealize Log Insight on-premise installation starting version 8.8. You can now forward logs from vRealize Log Insight (on-premise) to vRealize Log Insight Cloud without the need to deploy any additional Cloud Proxies.
- **Regional Log Support for Canada (Preview):** VMware Cloud on AWS SDDCs can now forward vRealize Log Insight Cloud logs to the Canada region, in addition to the Asia-Pacific (Sydney), Europe (Frankfurt), and US West (Oregon) regions. Once applied, this configuration becomes an organization-level change and all the SDDC logs point to the new region. You can select only one vRealize Log Insight Cloud region for an organization. To enable this feature, open a Service Request or chat with Support.

What's New March 2022

10

- **Usage Reports (Queries):** Usage reports have been enhanced to include the **Queries** tab. This tab contains log search (query) information such as the log volume scanned, total number of queries executed, and number of unique users executing queries. You can view charts with details about the logs examined over time, the number of queries executed over time, and so on.
- **Dark Theme:** You can now switch visual themes to view the thematic interface that you prefer. Click the **SWITCH THEME** option in the left navigation bar to switch between Light and Dark themes.
- **VMware NSX Advanced Load Balancer (by Avi Networks) Content Pack**: Enhanced key extraction regex for updated log formats.
- **New Region - Asia Pacific (India)**: vRealize Log Insight Cloud is now available in the AWS Asia Pacific (Mumbai) region, in addition to the AWS Asia Pacific (Tokyo), US(Oregon), Asia-Pacific (Singapore), Asia-Pacific (Sydney), Europe (Frankfurt), Europe (London), South America (Sao Paulo) and Canada(Toronto) regions.

What's New February 2022

11

- **Log Partition General Availability (GA):** Log partitions are now available as a GA feature. Log partitions provide a no-limit logging solution at low costs and eliminate any storage management overheads of the past. You can now archive logs for up to 7 years to meet your long-term retention requirements, which enables easy accessibility to archived logs by letting you run queries on demand. See the vRealize Log Insight pricing document for information about the NEW flexible pricing.
- **Usage Reports:** Through usage reports, you can view your vRealize Log Insight Cloud account usage volume at a glance. You get an overview of the daily ingestion, monthly ingestion, monthly indexed storage, monthly non-indexed storage, volume distribution by log partition, and daily usage trend chart.
- **Cloud Native Collector:** The Cloud Native Collector provides log collection and log aggregation for cloud native apps. You can install the Cloud Native Collector on an AWS EC2 instance, an Azure VM, or a Google Cloud Platform (GCP) VM instance and configure it to forward logs to vRealize Log Insight Cloud.

What's New December 2021

12

- **Log Forwarding System Alerts:** You can now configure email notifications to receive the following log forwarding errors:
  - Log Forwarding Deactivated Temporarily - Log forwarding is temporarily deactivated for the next few minutes. Too many log forwarding failures have been detected for the configured endpoint.
  - Log Forwarding Deactivated - Log forwarding is deactivated for the configured endpoint due to the inability to establish a connection.
- **Log Collection File Upload:** You can now use the simplified log file upload option to upload log files from your local system to vRealize Log Insight Cloud. You can upload up to 10 files of 10 MB each at any given time. The supported file formats for log upload are .log and .txt. This feature lets you quickly visualize Explore Logs, dashboards, alerts, and other capabilities with ease.
- **AWS Lambda and HashiCorp Vault Integration :** vRealize Log Insight Cloud uses a lambda function *VMware-Log-Insight-Cloud*to push logs from AWS CloudWatch, CloudTrail, and many other services to vRealize Log Insight Cloud. If you want to avoid storing vRealize Log Insight Cloud credentials in AWS Lambda functions, you can now configure to read a secret from the HashiCorp Vault Integration.
- **SSL Support for Cloud Proxy**: A Cloud Proxy receives log and event information from monitored sources and sends this information to vRealize Log Insight Cloud where it can be queried and analyzed. You can now configure your log sources to forward logs over SSL to the Cloud Proxy.
- **New Region - Asia Pacific (Japan)**: vRealize Log Insight Cloud is now available in the AWS Asia Pacific (Tokyo) region, in addition to the US(Oregon), Asia-Pacific (Singapore), Asia-Pacific (Sydney), Europe (Frankfurt), Europe (London), South America (Sao Paulo) and Canada(Toronto) regions.

What's New November 2021

13

- **Audit Events for VMware Cloud Services Content Pack:** This content pack is enhanced to include the Governance aspect of CSP. The following new charts are included with version 2.0 of the content pack:
  - Access Request Raised by Org Members
  - Access Request Raised by Non Org Members
  - Entitlement Request for Org Member Cancelled
  - Entitlement Request for Non Org Member Cancelled
  - Entitlement Request Actions
  - Entitlement Request Approval Actions
  - Violation Policies Updated
  - Entity Violations Count Update OAuth App
  - Entity Violations Count Update API Token
  - Advance Features Toggled

What's New October 2021

14

- **Alerts and Notifications:** You can now customize an alert definition to include extracted fields from logs in the alert title and description. When triggered, the alert sends out a notification to the configured endpoints (email and webhook). Additionally, you can add the following data associated with the alert to the notification.
  - Tags
  - All logs or extracted fields (JSON or table format)
  - Key-value data
- **Azure Network Watcher Content Pack:** A Network Security Group (NSG) contains security rules that allow or deny inbound network traffic to, or outbound network traffic from several types of Azure resources. This content pack is enhanced to support NSG logs and include dashboards that provide insights around the network activity to and from your NSGs.

What's New September 2021

15

- **Log Partitions (Beta):** Use vRealize Log Insight Cloud's petabyte scale and index-free log offering to meet your enterprise log management needs such as long-term storage and infrequent access. Indexed and index-free partition types let you divide data into value groups and define variable retention for better data and cost management. Going forward with log partitions, you can avail flexible pricing and usage monitoring. Log ingestion into index-free partitions supports:
  - Queries (Explore Logs)
  - Live Tail
  - Metric Extraction
  - Log Processing (Filter, Mask, and Tag Logs)
  - Log Retention (up to 7 years)
  - Log Forwarding
- **In-Product Guides:** In-product guides provide a step-by-step walkthrough on how to configure different features available in vRealize Log Insight Cloud. These guided tours include:
  - Adding Log Sources
  - vSphere Integration
  - Content Pack Installation
  - Dashboard Creation
  - Webhook Configuration
  - Alert Creation
  - Log Forwarding
  - Log Partitions

- **NSX-T Events for VMware Cloud SDDC Content Pack:** This content pack provides powerful insights into the NSX-T firewall rules and packet traffic rules created in VMware Cloud SDDC, along with audit details. These details let administrators audit, monitor, and troubleshoot the behavior of configured rules in their VMware Cloud SDDC environment. NSX-T 5.0 with Layer 7 security reveals Intrusion Detection and lets Prevention System users do a real-time analysis of log data for investigation, incident response, and forensics of security threats. The content pack is enhanced to include the following dashboards:
  - Traffic Dashboard
    - Top Signature Hits
    - Top Threats
    - Threats Over Time
    - Threats by Severity
    - Top Sources
    - Top Targets
    - Top Threats Category
  - Overview Dashboard
    - Policy Create/Update Events
    - Policy Delete Events
    - Policy Audit Events

What's New August 2021

16

- **Regional Log Support for Frankfurt and Sydney (Preview):** VMware Cloud on AWS SDDCs can now forward vRealize Log Insight Cloud logs to the Asia-Pacific (Sydney) and Europe (Frankfurt) regions, in addition to the US West (Oregon) region. Once applied, this configuration becomes an organization-level change and all the SDDC logs point to the new region. You can select only one vRealize Log Insight Cloud region for an organization. To enable this feature, open a Service Request or Chat with Support.
- **New Region - London and Sao Paulo**: vRealize Log Insight Cloud is now available in the AWS Europe (London) and South America (Sao Paulo) region, in addition to the US, Asia-Pacific (Singapore), Asia-Pacific (Sydney), Europe (Frankfurt), and Canada regions.
- **Search Text Box for Log Configuration Rules:** Under **Log Management**, you can now search for and filter configuration rules such as log forwarding, log archiving, and log processing.
- **Live Tail General Availability (GA):** Live tail is now available as a GA feature. For a detailed overview, see the live tail blog post.
- **Legends in Dashboards:** You can now view legends in dashboard widgets such as pie chart and donut. These legends are filterable and let you apply an inclusion or exclusion filter for the associated data.
- **Self-Service Subscription:** You can now use the **Subscriptions** page to view your subscription status for vRealize Log Insight Cloud and purchase or upgrade to a one or three-year commit model seamlessly.

What's New July 2021

17

- **New Region - Singapore:** vRealize Log Insight Cloud is now available in the AWS Asia-Pacific (Singapore) region, in addition to the US, Asia-Pacific (Sydney), Europe (Frankfurt), and Canada regions. Regional support for VMware Cloud on AWS is currently on the VMware Cloud on AWS roadmap.
- **Enhanced Log Forwarding Filter:** Log forwarding from vRealize Log Insight Cloud now supports additional filter options for whether a field exists or not, in addition to existing filter options for whether a field name contains or does not contain specific values. You can specify these filter conditions to select which events are forwarded to an external destination.
- **SDDC Grouping Activity Logs for VMware Cloud:** You can now access all your VMware Cloud SDDC Grouping activity logs in vRealize Log Insight Cloud. These logs correspond to the following activities:
  - Creation of an SDDC Group
  - Modification of an SDDC Group
  - Removal of an SDDC Group
  - Addition of an SDDC Member to a Group
  - Removal of an SDDC Member from a Group
  - Addition of a Direct Connect Gateway to a Group
  - Removal of a Direct Connect Gateway from a Group
  - Addition of an External AWS Account
  - Removal of an External AWS Account
  - Modification of External Attachments

What's New June 2021

18

For a detailed overview of the June 2021 release updates for vRealize Log Insight Cloud, see https://blogs.vmware.com/management/2021/06/vrealize-log-insight-cloud-june-2021-release.

- **Live Tail (Beta):** You can now stream log files and view them in real time as they are ingested into vRealize Log Insight Cloud. You can switch between the **Live Tail** and **Explore Logs** pages in the context of search for better troubleshooting. Live tail lets you:
  - Search and browse in context and use saved or favorite queries
  - Use out-of-the-box fields such as source, filepath, and so on
  - Highlight search texts or keywords
  - Pause and resume the live stream
- **Public Cloud Content Packs:** The following content packs are now available for **AWS** and **Azure** cloud services with a rich set of out-of-the-box content such as dashboards and queries.
  - AWS - AppConfig, Athena, CloudSearch, CloudTrail, CloudWatch, CodeCommit, Config, DocumentDB, DynamoDB, ElasticBeanstalk, ElasticCache, ElasticSearch, Inspector, RDS, Redshift, Route 53, S3, SNS, and SQS
  - Azure - Active Directory, App Service, Blob Storage, Event Hub, Function App, Kubernetes Service, Network Watcher, Search Service, Service Bus, and SQL

What's New May 2021

19

- **Knowledge Base (KB) Insights:** You can now browse and view the VMware knowledge base such as KB articles and community solutions for log events with errors or exceptions, and take actions to resolve them. KB insights use sophisticated machine learning techniques to help detect and associate log errors or events with suggested solutions from a knowledge base created by experts for similar problems solved in the past. For more information, see https://blogs.vmware.com/management/2021/05/introducing-vrealize-log-insight-cloud-kb-insights.html.
- **What's New:** A new user-friendly What’s New pop-up window now provides information about the latest features in vRealize Log Insight Cloud.

What's New February 2021

20

- **Rsyslog Log Source:** You can now configure Rsyslog to collect logs from your host, containers, and services, and forward them to vRealize Log Insight Cloud. You can find the configuration steps within the vRealize Log Insight Cloud user interface.
- **Google Cloud Platform (GCP) Cloud Content Packs:** The following content packs are now available with a rich set of out-of-the-box content.
  - App Engine
  - Big Query
  - Cloud Foundation
  - Cloud SQL
  - Cloud Storage
  - Compute Engine
  - Firewall
  - Identity and Access Management (IAM)
  - Kubernetes
  - Load Balancing
  - Virtual Private Cloud (VPC)

What's New January 2021

21

- **Logstash Log Source:** You can now configure Logstash to collect logs from various sources and forward them to vRealize Log Insight Cloud. Logstash is an open source data collection engine with real-time pipelining capabilities. You can find the configuration steps within the vRealize Log Insight Cloud user interface.
- **Alert Definition:** The new alert management UI lets you create a granular rule definition of log alerts/events with the ability to set different notifications for different severities. The **Alert Definition** options let you browse all the log alert definition rules at one place. You can sort them through text filters or by origin, type, and tags. You can select multiple rules and take actions quickly like add or remove tags, add to a dashboard, or delete them . You can also classify alerts as info, warning, immediate, or critical, and change your notification methods as required.
- **Alert Exploration:** You can browse your security incidents and log alerts similar to log search with the new **Triggered Alerts** page. You can filter triggered alerts by severity, type, origin, and tags for quick review and prioritization. The new alert notifications include chart visualizations of triggered alerts over a specified time range.
- **VMware Site Recovery Manager Log Integration:** VMware Site Recovery Manager (SRM) is a business continuity and disaster recovery solution that helps you plan, test, and run the recovery of virtual machines between a protected vCenter Server site and a recovery vCenter Server site. SRM log integration and content pack is now available, which collects, imports, and analyzes logs to provide real-time answers to problems related to systems, services, and applications, and derive important insights.

What's New December 2020

22

- **GCP Log Sources:** vRealize Log Insight Cloud provides 11 Google Cloud Platform log sources, including applications such as CloudFunctions, Compute Engine, Firewall, Storage, and VPC. You can find the configuration steps for the log sources within the user interface. Once the logging configuration is complete, you can verify the log flow to the environment in **Log Sources**, on the **Logs** tab. The log messages already include the field definitions in the log stream to assist with log filtering and alerting. Administrators can also extract custom field definitions.
- **Fluent Bit Log Source:** You can now configure Fluent Bit to collect logs from various sources and forward to vRealize Log Insight Cloud. Fluent Bit is an open source Log Processor and Forwarder, which lets you collect data like logs from different sources and enrich them with filters. It is the preferred choice for containerized environments such as Kubernetes. You can find the configuration steps for the Fluent Bit log sources within the vRealize Log Insight Cloud user interface.
- **New Region: EU (Frankfurt):** vRealize Log Insight Cloud is now available in the AWS EU (Frankfurt) region.

What's New October 2020

23

- **Azure Log Sources:** vRealize Log Insight Cloud provides 11 Azure Cloud log sources, including applications such as Activity Logs, Blob Storage, Event Hub, Kubernetes Service, Search Service, and SQL. You can find the configuration steps for the log sources within the vRealize Log Insight Cloud user interface. Once the logging configuration is complete, you can verify the log flow to the environment in **Log Sources**, on the **Logs** tab. The log messages already include the field definitions in the log stream to assist with log filtering and alerting. Administrators can also extract custom field definitions.
- **New AWS Log Sources:** vRealize Log Insight Cloud now provides 41 AWS log sources, including newly added applications such as CodeBuild, Code Deploy, EBS, EventBridge, and Fargate.

What's New September 2020

24

- **New Region - APJ (Sydney):**vRealize Log Insight Cloud is now available in the AWS APJ (Sydney) region.
- **vRealize Log Insight Cloud from VMware Cloud on AWS Activity Log:** You can now access vRealize Log Insight Cloud from the Activity Log through a quick link to view all your logs, including all the events in your Activity Log.

What's New August 2020

25

For a detailed overview of the August 2020 release updates for vRealize Log Insight Cloud, see https://blogs.vmware.com/management/2020/09/vmware-vrealize-log-insight-cloud-q3-release-updates.html.

- **AWS Log Sources:** vRealize Log Insight Cloud provides 35 AWS log sources, including applications such as CloudTrail, CodeDeploy, and SQS. You can find the configuration steps for the log sources within the user interface. Once the logging configuration is complete, you can verify the log flow to the environment in **Log Sources**, on the **Logs** tab. vRealize Log Insight Cloud includes out-of-the-box dashboards for AWS services including DynamoDB, Kinesis, S3, SNS, SQS, and EKS. The log messages already include the field definitions in the log stream to assist with log filtering and alerting. Indexed fields are created based on intelligent grouping algorithms applied to messages that are ingested. Content fields are defined as part of content packs that are enabled. Administrators can also extract custom field definitions.
- **One-Click Field Extraction:** vRealize Log Insight Cloud includes a number of extracted fields based on log sources and content packs. The one-click extract field option populates all context values that correspond to the field you select in a log event in a case where you want to assign values to log data that is not already extracted. You can review extracted field regex values that were automatically defined.
- **Home Page Customization:** vRealize Log Insight Cloud has a customizable **Home** page with a drag-and-drop functionality that lets you add widgets to the page. You can also set a dashboard as the landing page, so that the dashboard is the first page you see when you sign in.
- **Dashboard Workbench:** vRealize Log Insight Cloud provides the interface for creating dashboards with a drag-and-drop functionality. You can add your most frequently used queries and alerts to your dashboards for quick review. You can also resize widgets and move them around the canvas as desired.
- **Dashboard Filtering with Group Actions:** The new dashboard management options let you quickly tag dashboards for specific service roles, sort dashboards through text filters, by content packs, or author. You can filter by your customized lists or by the number of widgets. You can select multiple dashboards and add them to lists, add or remove tags, or delete them. You can manage thousands of dashboards by using filters.

- **Audit Events for VMware Cloud:** You can access all your VMware Cloud audit events including Activity Overview, Alarms, Clusters, Datastores, DRS, Hosts, NSX-T Events, Resource Pools, Roles and Permissions, Users, and Virtual Machines. You can quickly access log data from a dashboard query.
- **Log Data Navigation from Dashboards:** You can review detailed log queries represented in dashboard widgets.
- **Comprehensive Overview Dashboard:** You can review events by type and host name, and review unique instances of event types occurring in your environment.
- **Alert Snoozing:** You can quickly deactivate alerts while troubleshooting a known issue or for scheduled maintenance.
- **Customize Visualizations:** You can modify chart types, including new options for Event Streams and Event Trends.