Série de Certificação GCP: 5.3 Visualizando logs de auditoria para o projeto e serviços gerenciados

Prashanta Paudel

14 de novembro de 2018 · 34 minutos de leitura

Conceitos básicos

O Stackdriver Logging faz parte do conjunto de produtos do Stackdriver no Google Cloud Platform (GCP). Ele inclui armazenamento para logs, uma interface de usuário chamada Visualizador de logs e uma API para gerenciar logs programaticamente. O registro em log permite ler e gravar entradas de registro, pesquisar e filtrar seus registros, exportar seus registros e criar métricas baseadas em registros.

Projetos

Os logs são associados principalmente a projetos do GCP, embora outros recursos, como organizações, pastas e contas de cobrança, também possam ter logs. O Logs Viewer mostra apenas os logs de um projeto, mas usando a API, você pode ler entradas de log em vários recursos.

Entradas de registro

Uma entrada de registro registra o status ou um evento. A entrada pode ser criada por serviços GCP, serviços da AWS, aplicativos de terceiros ou seus próprios aplicativos. A “mensagem” que a entrada de log transporta é chamada de carga útil e pode ser uma string simples ou dados estruturados.

Seu projeto recebe entradas de registro quando você começa a usar os serviços que rotineiramente produzem entradas de registro, como o Compute Engine ou o BigQuery. Você também recebe entradas de registro quando conecta o Stackdriver à AWS, quando instala o agente

de registro em suas instâncias de VM e quando liga para as entradas. escreva o método na API.

Logs

Um log é uma coleção nomeada de entradas de log dentro de um recurso do GCP. Cada entrada de log inclui o nome do seu log. Um nome de log pode ser um simples identificador, como `syslog`, ou um nome estruturado incluindo o autor do log, como `compute.googleapis.com/activity`. Os logs existem somente se tiverem entradas de log.

Período de retenção

As entradas de log são mantidas no Stackdriver Logging por um tempo limitado conhecido como período de retenção. Depois disso, as entradas são apagadas. Se você quiser manter suas entradas de log por mais tempo, exporte-as para fora do Stackdriver Logging.

Os períodos de retenção para diferentes tipos de logs são listados na Política de Cota de Registro .

Recursos monitorados

Cada entrada de log indica de onde veio incluindo o nome de um recurso monitorado. Exemplos são instâncias individuais de VMs do Compute Engine, instâncias individuais de VMs do Amazon EC2, instâncias de bancos de dados e assim por diante. Para obter uma listagem completa dos tipos de recursos monitorados, consulte Recursos e Serviços Monitorados .

Filtros

Um filtro de registros avançados é uma expressão no idioma do filtro de registro. Ele é usado no Visualizador de registros e na Stackdriver Logging API para selecionar entradas de registro, como aquelas de uma determinada instância de VM ou aquelas que chegam em um período de tempo específico com um determinado nível de gravidade.

Exportando logs usando coletores

As entradas de registro recebidas pelo registro podem ser exportadas para os intervalos do Cloud Storage, conjuntos de dados do BigQuery e tópicos do Cloud Pub / Sub. Você exporta logs configurando os coletores de log, que continuam exportando as entradas de registro à medida que chegam ao registro. Um coletor inclui um destino e um filtro que seleciona as entradas de log para exportar.

Métricas baseadas em registros

As métricas são um recurso do Stackdriver Monitoring. Uma métrica baseada em registros é uma métrica cujo valor é o número de entradas de log que correspondem a um filtro especificado por você.

Registros de auditoria

Um log de auditoria é um log permanente gravado por um serviço do GCP para registrar ações administrativas ou do usuário. Registros de auditoria aparecem no Visualizador de registros junto com outros registros. Para mais informações, consulte Logs de auditoria .

Controle de acesso

A capacidade de ler registros de log é controlada pela concessão de permissões de gerenciamento de identidade e acesso ao Cloud aos membros.

A maioria dos registros pode ser lida por qualquer membro com a função Cloud IAM **Viewer** . Os registros de auditoria de acesso a dados , exceto os logs de auditoria do BigQuery Data Access, são os únicos "registros privados". Para lê-los, o membro precisa da função de proprietário do Cloud IAM ou de outras permissões especiais

- ++++++++++++++++++++++++++++++++++

Guia de Controle de Acesso

O Stackdriver Logging usa o Cloud Identity e o Access Management para controlar o acesso a dados de registro em projetos, organizações, pastas e contas de faturamento.

visão global

As permissões e funções do Cloud IAM determinam como você pode usar a API de registro e o Visualizador de registros .

Uma função do Cloud IAM é uma coleção de permissões. Você atribui essas funções aos membros . Você não pode atribuir uma permissão a um membro diretamente; em vez disso, você concede a eles uma função, que concede a eles todas as permissões que a função contém.

Os dados de log residem nesses tipos de recursos: projetos, organizações, pastas e contas de faturamento. Cada um desses recursos pode ter seu próprio conjunto de membros com seus próprios conjuntos de funções de registro em log.

Para criar ou usar dados de registro do Stackdriver Logging em um recurso, um membro deve ter uma função do Cloud IAM que inclua as permissões apropriadas. Uma lista resumida dessas funções e permissões do Cloud IAM é mostrada abaixo:

- **roles / logging.viewer** (Logs Viewer) fornece aos membros acesso somente leitura a todos os recursos do Log, exceto a permissão para ler logs privados.
- **roles / logging.privateLogViewer** (Private Logs Viewer) fornece aos membros as permissões encontradas em **roles / logging.viewer** , além da permissão para ler logs privados.
- **roles / logging.logWriter** (Logs Writer) pode ser concedido a membros que são contas de serviço e fornece aos membros apenas permissões suficientes para gravar logs. Esta função não concede acesso ao Visualizador de registros.
- **roles / logging.configWriter** (Gravador de configuração de logs) fornece aos membros as permissões para criar métricas baseadas em logs e exportar coletores. Para usar o Visualizador de registros, adicione a **função roles / logging.viewer** .
- **roles / logging.admin** (Logging Admin) fornece aos membros todas as permissões relacionadas ao registro em log. Para obter uma lista completa dessas permissões, consulte Permissões da API .
- **roles / viewer** (Project Viewer) fornece aos membros as mesmas permissões que **roles / logging.viewer** no nível do projeto.

Observe que a concessão dessa função aplica as permissões à maioria dos serviços do GCP no nível do projeto e não se limita ao uso de registro em log.

- **roles / editor** (Editor de Projetos) fornece aos membros as mesmas permissões que **roles / logging.viewer** , além de permissões para gravar entradas de log, excluir logs e criar métricas baseadas em logs, no nível do projeto. A função não permite criar coletores de exportação ou ler logs privados. Observe que a concessão dessa função aplica as permissões à maioria dos serviços do GCP no nível do projeto e não se limita ao uso de registro em log.
- **roles / owner** (Project Owner) fornece acesso total ao registro, incluindo registros privados. Observe que a concessão dessa função aplica as permissões à maioria dos serviços do GCP no nível do projeto e não está restrita ao uso do registro em log.

Os registros de auditoria de acesso a dados , exceto os logs de auditoria do BigQuery Data Access, são os únicos "registros privados". Para lê-los, os membros exigem certas permissões que são mais amplas que as permissões somente leitura.

Para obter mais detalhes sobre funções e permissões de log, consulte Permissões e funções nesta página.

Permissões da API

Os métodos da API de registro exigem permissões específicas do Cloud IAM. A tabela a seguir lista as permissões necessárias pelos métodos da API.

Observação: se você estiver interessado em registros mantidos em organizações, contas de faturamento e pastas, observe que esses recursos têm seus próprios métodos de API para `logs` e `sinks` . Em vez de repetir todos os métodos da tabela, apenas os `projects` métodos são mostrados individualmente.

Logging methodRequired permissionResource type `billingAccounts.logs.*`logging.logs.*(Consulte `projects.logs.*`) contas de faturamento `billingAccounts.sinks.*`logging.sinks.* (consulte `projects.sinks.*` .) Contas

`entries.list` `logging.logEntries.list` ou `logging.privateLogEntries.list` projetos de cobrança , organizações, pastas, `entries.write` `logging.logEntries.create` projetos de contas de faturamento , organizações, pastas, contas de faturamento `folders.logs.*` `logging.logs.*` (Ver `projects.logs.*`) pastas `folders.sinks.*` `logging.sinks.*` (Ver `projects.sinks.*`) pastas `monitoredResourceDescriptors.list` (nenhuma) (nenhuma) `organizations.logs.*` `logging.logs.*` (Ver `projects.logs.*`) organizações `organizations.sinks.*` `logging.sinks.*` (Veja `projects.sinks.*`) organizações `projects.exclusions.create` `logging.exclusions.create` projeta `projects.exclusions.delete` `logging.exclusions.delete` projetos `projects.exclusions.get` `logging.exclusions.get` projeta `projects.exclusions.list` `logging.exclusions.list` projetos `projects.exclusions.patch` `logging.exclusions.<b>update<b>` projeta `projects.logs.list` `logging.logs.list` projetos `projects.logs.delete` `logging.logs.delete` projeta `projects.sinks.list` `logging.sinks.list` projetos `projects.sinks.get` `logging.sinks.get` projeta `projects.sinks.create` `logging.sinks.create` projetos `projects.sinks.update` `logging.sinks.update` projeta `projects.sinks.delete` `logging.sinks.delete` projetos `projects.metrics.list` `logging.logMetrics.list` projeta `projects.metrics.get` `logging.logMetrics.get` projetos `projects.metrics.create` `logging.logMetrics.create` projeta `projects.metrics.update` `logging.logMetrics.update` projetos `projects.metrics.delete` `logging.logMetrics.delete` projetos

Permissões e papéis

A tabela a seguir lista as funções do Cloud IAM que concedem acesso ao Stackdriver Logging. Cada função tem um conjunto específico de permissões de registro. As funções podem ser atribuídas a membros dos tipos de recursos listados.

Na tabela, `a.b.{x,y}` significa `a.b.x` e `a.b.y` .

Role nameRole titleLogging permissionsResource type `roles/logging.viewer` Visualizador de logs `logging.logEntries.list` `logging.logMetrics.` { `list` , `get` }

`logging.logs.list`
`logging.logServiceIndexes.list`
`logging.logServices.list`
`logging.sinks.` { `list` , `get` }
`logging.usage.get`
`resourcemanager.projects.get` projeto, organização,
pasta, conta de faturamento `roles/`
`logging.privateLogViewer` Private Logs
`roles/logging.viewer` Permissões do visualizador mais:
`logging.privateLogEntries.list` projeto, organização,
pasta, conta de faturamento `roles/`
`logging.logWriter` Logs Writer `logging.logEntries.create` project,
organização,
pasta, conta de faturamento `roles/`
`logging.configWriter` Logs Configuration Writer
`logging.exclusions.` { `list` , `create` , `get` , `update` , `delete` }
`logging.logMetrics.` { `list` , `create` , `get` , `update` , `delete` }
`logging.logs.list`
`logging.logServiceIndexes.list`
`logging.logServices.list`
`logging.sinks.{list` , `create` , `get` , `update` , `delete` }
`resourcemanager.projects.get` projeto, organização,
pasta, conta de cobrança `roles/`
`logging.admin` Logging administrador `logging.exclusions.` { `list` ,
`create` , `get` , `update` , `delete` }
`logging.logEntries.create`
`logging.logEntries.list`
`logging.logMetrics.` { `list` , `create` , `get` , `update` , `delete` }
`logging.logs.delete`
`logging.logs.list`
`logging.logServiceIndexes.list`
`logging.logServices.list`
`logging.privateLogEntries.list`
`logging.sinks.{list` , `create` , `get` , `update` , `delete` }
`resourcemanager.projects.get` Projeto, organização,
pasta, conta de cobrança `roles/viewer` Visualizador
`logging.logEntries.list`
`logging.logMetrics.` { `list` , `get` }
`logging.logs.list`
`logging.logServiceIndexes.list`
`logging.logServices.list`

`logging.sinks.` { `list` , `get` }
`resourcemanager.projects.get` projeto `roles/editor` Editor de
`roles/viewer` permissões de Registro, mais:
`logging.logEntries.create`
`logging.logMetrics.` { `create` , `update` , `delete` }
`logging.logs.delete` projeto `roles/owner` proprietário
`roles/editor` permissões de Registro, mais:
`logging.privateLogEntries.list`
`logging.sinks.` { `create` , `update` , `delete` } projeto

Papéis personalizados

Para criar uma função personalizada com permissões de log, faça o seguinte:

- Para uma função concedendo permissões apenas para a API de registro, escolha entre as permissões na seção anterior, permissões da API .
- Para uma função que concede permissões para usar o Visualizador de Logs, escolha entre os grupos de permissões na seção a seguir, Permissões do Console .

Para mais informações sobre funções personalizadas, consulte Noções básicas sobre funções personalizadas do Cloud IAM .

Permissões do console

A tabela a seguir lista as permissões necessárias para usar o Visualizador de registros .

Na tabela, `a.b.{x,y}` significa `a.b.x` e `a.b.y` .

Console activityRequired permissionsMinimal somente leitura acessar
`logging.logEntries.list`
`logging.logs.list`
`logging.logServiceIndexes.list`
`logging.logServices.list`
`resourcemanager.projects.get` Adicionar capacidade de visualizar os registos à base de metricsAdd `logging.logMetrics.` { `list` , `get` } Adicionar capacidade de visualizar exportsAdd `logging.sinks.` { `list` , `get` } Adicionar capacidade de exibir logs usageAdd

`logging.usage.get` Adicionar capacidade de excluir logsAdd `logging.exclusions.` { `list` , `create` , `get` , `update` , `delete` } Adicionar capacidade de exportar logsAdd `logging.sinks.{list` , `create` , `get` , `update` , `delete` } Adicionar capacidade de criar metricsAdd registros baseada em `logging.logMetrics.` { `list` , `create` , `get` , `update` , `delete` }

Acesso a logs exportados

Para criar um coletor , para exportar logs, você deve ter as permissões de `roles/logging.configWriter` ou `roles/logging.admin` ou `roles/owner` .

Depois que um coletor começa a exportar registros, ele tem acesso total a todas as entradas de registro de entrada. Os coletores podem exportar entradas de registro privadas.

Depois que as entradas de registro forem exportadas, o acesso às cópias exportadas será totalmente controlado pelas permissões e funções do Cloud IAM nos destinos: Cloud Storage, BigQuery ou Cloud Pub / Sub.

Explorando escopos de acesso

Os escopos de acesso são o método legado de especificar permissões para suas instâncias de VM do Compute Engine. Os escopos de acesso a seguir se aplicam à API de registro:

Acesse scopePermissions grantedhttps: //www.googleapis.com/auth/logging.read `role/logging.viewer` https://www.googleapis.com/auth/logging.write `roles/logging.logWriter` https://www.googleapis.com/auth/logging.adminFull access to the API de registro.https: //www.googleapis.com/auth/cloud-platformAcesso completo à API de registro e a todas as outras APIs do Google Cloud ativadas.

Melhores práticas

Agora que as funções do Cloud IAM estão disponíveis, uma prática razoável é dar a todas as suas instâncias de VM o escopo "Acesso total a todas as APIs do Google Cloud ativas":

```
https://www.googleapis.com/auth/cloud-platform
```

Você pode conceder funções específicas do Cloud IAM na conta de serviço da sua instância de VM para restringir o acesso a APIs específicas. Para detalhes, consulte Permissões da conta de serviço .

++++++++++++++++++++++++++++++++++

Usando Logs Exportados

Esta página explica como você pode encontrar e usar suas entradas de registro exportadas no Cloud Storage, no BigQuery e no Cloud Pub / Sub.

Para obter uma visão geral dos registros de exportação, consulte Visão geral da exportação de logs .

Para saber como exportar seus registros, consulte as seguintes páginas:

- Para usar o Visualizador de registros, consulte Exportando registros .
- Para usar a Stackdriver Logging API, consulte Exportando registros na API .
- Para usar a ferramenta de linha de comando, consulte gcloud logging .

Armazenamento na núvem

Para ver seus registros exportados no Cloud Storage, faça o seguinte:

1. Vá para o navegador do Cloud Storage no Console do GCP:
2. NAVEGADOR DE ARMAZENAMENTO EM NUVEM
3. Selecione o bucket que você está usando para exportar logs.

Consulte a organização do Cloud Storage para obter detalhes sobre como os registros são organizados no intervalo.

Disponibilidade de registros exportados

Se você não vir nenhum log exportado, verifique as métricas do sistema de exportação . As métricas do sistema de exportação podem informar quantas entradas de log são exportadas e quantas são descartadas devido a erros. Se as métricas do sistema de exportação indicarem que nenhuma entrada de registro foi exportada, verifique seu filtro de exportação para verificar se as entradas de registro correspondentes ao seu filtro chegaram recentemente ao Stackdriver Logging:

IR PARA A PÁGINA DE EXPORTAÇÃO DE LOGS

As entradas de registro são salvas nos intervalos do Cloud Storage em lotes por hora. Pode levar de 2 a 3 horas para que as primeiras entradas comecem a aparecer.

Organização de registros exportados

Quando você exporta registros para um intervalo do Cloud Storage, o Stackdriver Logging grava um conjunto de arquivos no intervalo. Os arquivos são organizados em hierarquias de diretório por tipo de registro e data. O tipo de log pode ser um nome simples como `syslog` ou um nome composto como `appengine.googleapis.com/request_log` . Se esses logs fossem armazenados em um bucket chamado `my-gcs-bucket` , os diretórios seriam nomeados como no exemplo a seguir:

```
my-gcs-bucket/syslog/YYYY/MM/DD/
my-gcs-
bucket/appengine.googleapis.com/request_log/YYYY/MM/DD/
```

Um único depósito pode conter logs de vários tipos de recursos.

O Stackdriver Logging não garante deduplicação de entradas de log de coletores que contêm filtros idênticos ou sobrepostos; As entradas de registro desses coletores podem ser gravadas várias vezes em um intervalo do Cloud Storage.

Os diretórios folha (`DD/`) contêm vários arquivos, cada um dos quais contém as entradas de log exportadas por um período de tempo

especificado no nome do arquivo. Os arquivos são *fragmentados* e seus nomes terminam em um número de fragmentos, `Sn` ou `An` (n = 0, 1, 2, ...). Por exemplo, aqui estão dois arquivos que podem ser armazenados no diretório `my-gcs-bucket/syslog/2015/01/13/` :

```
08: 00: 00_08: 59: 59_S0.json
08: 00: 00_08: 59: 59_S1.json
```

Esses dois arquivos juntos contêm as `syslog` entradas de log para todas as instâncias durante a hora a partir de 08:00 UTC. Os registros de data e hora de entrada de log são expressos em UTC (Tempo Universal Coordenado).

Para obter todas as entradas de log, você deve ler todos os fragmentos para cada período de tempo - nesse caso, os shards 0 e 1. O número de fragmentos de arquivos gravados pode mudar para cada período de tempo, dependendo do volume de entradas de log.

Nos arquivos individuais particionados, as entradas de log são armazenadas como uma lista de `LogEntry` objetos. Para uma `syslog` entrada de exemplo , consulte LogEntry type nesta página.

Observe que a ordem de classificação das entradas de log nos arquivos não é uniforme ou de outra forma garantida.

BigQuery

Para ver seus registros exportados no BigQuery, faça o seguinte:

1. Vá para a interface do BigQuery no console do GCP:
2. IR PARA A BIGQUERY UI
3. Selecione o conjunto de dados usado como o destino do seu coletor.
4. Selecione uma das tabelas do conjunto de dados. As entradas de log são visíveis na guia **Detalhes** ou você pode consultar a tabela para retornar seus dados.

Para obter mais informações, consulte Organização de tabelas para saber como as tabelas são organizadas e Exportar registros e o esquema do BigQuery para saber como os campos de entrada do registro exportados são nomeados.

Disponibilidade do BigQuery

Se você não vir nenhum log exportado, verifique as métricas do sistema de exportação . As métricas do sistema de exportação podem informar quantas entradas de log são exportadas e quantas são descartadas devido a erros. Se as métricas do sistema de exportação indicarem que nenhuma entrada de registro foi exportada, verifique seu filtro de exportação para verificar se as entradas de registro correspondentes ao seu filtro chegaram recentemente ao Stackdriver Logging:

IR PARA A PÁGINA DE EXPORTAÇÃO DE LOGS

As entradas de log são salvas no BigQuery em lotes. Pode levar vários minutos até que as primeiras entradas comecem a aparecer.

Organização de tabelas

Quando você exporta registros para um conjunto de dados do BigQuery, o Stackdriver Logging cria tabelas com datas para conter as entradas do registro exportadas. As entradas de registro são colocadas em tabelas cujos nomes são baseados nos nomes de registros e registros de data e hora das entradas1. A tabela a seguir mostra exemplos de como nomes de log e registros de data e hora são mapeados para nomes de tabelas:

Registro do nome do registro de log timestamp1BigQuery table namesyslog2017–05–23T18: 19: 22.135Zsyslog_20170523apache-access2017–01–01T00: 00: 00.000Zapache_access_20170101compute.googleapis.com/activity_log2017–12–31T23: 59: 59.999Zcompute_googleapis_com_activity_log_20171231

1: Os timestamps de entrada de log são expressos em UTC (Tempo Universal Coordenado).

Esquemas e campos

Os esquemas de tabela do BigQuery para logs exportados são baseados na estrutura do tipo LogEntry e no conteúdo das cargas de log. Você pode ver o esquema da tabela selecionando uma tabela com entradas de registro exportadas na interface da Web do BigQuery .

O esquema de tabela do BigQuery usado para representar cargas de entrada de log complexas pode ser confuso e, no caso de logs de auditoria exportados, algumas regras de nomenclatura especiais são usadas. Para mais informações, consulte Esquema do BigQuery de registros exportados .

Consultas

Observação: as exportações de registros de auditoria para o BigQuery agora apresentam um formato compacto. **Em 1º de março de 2019, o esquema mais antigo será removido** . Se você não exportar registros de auditoria para o BigQuery, não será afetado por essa alteração. Os usuários que exportam logs de auditoria para o BigQuery devem examinar os campos alterados e atualizar as consultas que os consomem. Para detalhes, consulte Migração para o esquema atualizado .

Para exemplos de consultas que envolvem registros de auditoria exportados no BigQuery, consulte as consultas de log de auditoria do BigQuery .

Consulte a Referência de consulta para mais informações sobre consultas do BigQuery. Especialmente úteis são as funções de caractere curinga de tabela , que permitem fazer consultas em várias tabelas e o operador Flatten , que permite exibir dados de campos repetidos.

Uma consulta de registros de amostra do Compute Engine

A consulta do BigQuery a seguir recupera entradas de log de vários dias e vários tipos de log:

- A consulta pesquisa os últimos três dias dos logs `syslog` e `apache-access` . A consulta foi feita em 23-Fev-2015 e abrange todas as entradas de log recebidas em 21-Fev e 22-Fev, além de entradas de log recebidas em 23-Fev até o momento em que a consulta foi emitida.

- A consulta recupera os resultados de uma única instância do Compute Engine `1554300700000000000` .
- A consulta ignora o tráfego do verificador de integridade do ponto final do Stackdriver Monitoring `Stackdriver_terminus_bot` ,.

```
SELECT
  timestamp AS Time,
  logName como Log,
  textPayload como Mensagem
FROM
  (TABLE_DATE_RANGE (my_bq_dataset.syslog_,
    DATE_ADD (CURRENT_TIMESTAMP (), -2, 'DAY'),
CURRENT_TIMESTAMP ())),
  (TABLE_DATE_RANGE (my_bq_dataset.apache_access_,
    DATE_ADD (CURRENT_TIMESTAMP) (), -2, 'DAY'),
CURRENT_TIMESTAMP ()))
WHERE
  resource.type == 'gce_instance'
  E resource.labels.instance_id == '1554300700000000000'
  E NOT (textPayload CONTÉM 'Stackdriver_terminus_bot')
ORDER BY time;
```

Aqui estão algumas linhas de saída de exemplo:

```
Row | Tempo | Log | Mensagem
--- | ---------------------- | ----------------------------
--------------- | ----------------------------------------
-------- ------------------------------------------------
------------
5 | 2015-02-21 03:40:14 UTC | projetos / project-id / logs /
syslog | Feb 21 03:40:14 my-gce-instance collectd [24281]:
uc_update: Valor muito antigo: name = 15543007601548826368 /
df-tmpfs / df_complex-used; valor tempo = 1424490014.269;
última atualização de cache = 1424490014.269;
6 | 2015-02-21 04:17:01 UTC | projetos / project-id / logs /
syslog | Feb 21 04:17:01 meu-gce-instance / USR / SBIN /
CRON [8082]: (raiz) CMD (cd / && run-parts --reportar
/etc/cron.hourly)
7 | 2015-02-21 04:49:58 UTC | projetos / id-project / logs /
apache-access | 128.61.240.66 - - [21 / Fev / 2015: 04: 49:
58 +0000] "GET / HTTP / 1.0" 200 536 "-" "masscan / 1.0
(https://github.com/robertdavidgraham/masscan)"
8 | 2015-02-21 05:17:01 UTC | projetos / project-id / logs /
syslog | 21 de fevereiro de 05:17:01 my-gce-instance / USR /
SBIN / CRON [9104]: (raiz) CMD (cd / && run-parts --reportar
/etc/cron.hourly)
9 | 2015-02-21 05:30:50 UTC | projetos / project-id / log /
syslogapache-access | 92.254.50.61 - - [21 / Fev / 2015: 05:
```

```
30: 50 +0000] "GET /tmUnblock.cgi HTTP / 1.1" 400 541 "-" "-
"
```

Uma consulta de registros de amostra do App Engine

A consulta do BigQuery a seguir recupera solicitações malsucedidas do App Engine do último mês:

```
SELECT
  timestamp AS Tempo,
  protoPayload.host AS Host,
  protoPayload.status Status AS,
  protoPayload.resource AS Caminho
FROM
  (TABLE_DATE_RANGE
(my_bq_dataset.appengine_googleapis_com_request_log_,
    DATE_ADD (CURRENT_TIMESTAMP (), -1, 'MÊS'),
CURRENT_TIMESTAMP ()))
WHERE
  protoPayload.status! = 200
ORDER BY time
```

Aqui estão alguns dos resultados:

```
Row | Tempo | Host | Status | Caminho
--- | ---------------------- | ----------------------------
--------- | ------ | ------
6 | 2015-02-12 19:35:02 UTC | default.my-gcp-project-
id.appspot.com | 404 | / foo thud = 3
7 | 2015-02-12 19:35:21 UTC | default.my-gcp-project-
id.appspot.com | 404 | / foo
8 | 2015-02-16 20:17:19 UTC | my-gcp-project-id.appspot.com
| 404 | /favicon.ico
9 | 2015-02-16 20:17:34 UTC | my-gcp-project-id.appspot.com
| 404 | / foo? thud =% 22what ???% 22
```

Cloud Pub / Sub

Para ver seus registros exportados enquanto eles são transmitidos por meio do Cloud Pub / Sub, faça o seguinte:

1. Vá para a página do Cloud Pub / Sub no console do GCP:

2. IR PARA NUVEM PUB / SUB
3. Localize ou crie uma assinatura para o tópico usado para exportação de logs e retire uma entrada de log dele. Talvez seja necessário aguardar a publicação de uma nova entrada de log.

Consulte Organização de registros exportados para obter detalhes sobre como os registros são organizados.

Disponibilidade de registros exportados

Se você não vir nenhum log exportado, verifique as métricas do sistema de exportação . As métricas do sistema de exportação podem informar quantas entradas de log são exportadas e quantas são descartadas devido a erros. Se as métricas do sistema de exportação indicarem que nenhuma entrada de registro foi exportada, verifique seu filtro de exportação para verificar se as entradas de registro correspondentes ao seu filtro chegaram recentemente ao Stackdriver Logging:

IR PARA A PÁGINA DE EXPORTAÇÃO DE LOGS

Quando você exporta registros para um tópico do Cloud Pub / Sub, o Stackdriver Logging publica cada entrada de log como uma mensagem do Cloud Pub / Sub assim que o Stackdriver Logging recebe essa entrada de registro.

Organização de registros exportados

O `data` campo de cada mensagem é um objeto LogEntry codificado em base64 . Por exemplo, um assinante do Cloud Pub / Sub pode extrair o seguinte objeto de um tópico que está recebendo entradas de log. O objeto mostrado contém uma lista com uma única mensagem, embora o Cloud Pub / Sub possa retornar várias mensagens se várias entradas de log estiverem disponíveis. O `data` valor (cerca de 600 caracteres) e o `ackId` valor (cerca de 200 caracteres) foram reduzidos para tornar o exemplo mais fácil de ler:

```
{
"ReceivedMessages": [
  {
   "ackId": "dR1JHlAbEGEIBERNK0EPKVgUWQYyODM ...
QlVWBwY9HFELH3cOAjYYFlcGICIjIg",
```

```
    "message": {
     "dados": "eyJtZXRhZGF0YSI6eyJzZXZ0eSI6Il ...
Dk0OTU2G9nIjoiaGVsbG93b3JsZC5sb2cifQ ==",
     "atributos": {
      "compute.googleapis.com/ resource_type ": "instância",
      "compute.googleapis.com/resource_id": "123456"
     },
     "messageId": "43913662360"
    }
   }
]
}
```

Se você decodificar o `data` campo e formatá-lo, você receberá o seguinte objeto LogEntry :

```
{
  "log": "helloworld.log",
  "insertId": "2015-04-15 | 11: 41: 00.577447-07 |
10.52.166.198 | -1694494956",
  "textPayload": "Qua Abr 15 20:40: 51 CEST 2015 Olá, mundo!
",
  " Timestamp ":" 2015-04-15T18: 40: 56Z ",
  " labels ": {
    " compute.googleapis.com \ / resource_type ":" instance
",
    " compute.googleapis. com \ / resource_id ":" 123456 "
  },
  " severity ":" AVISO "
  }
}
```

Objetos de entrada de log

As entradas de log do Stackdriver Logging são objetos do tipo LogEntry . Os campos mais importantes da entrada de log são mostrados na tabela a seguir:

É costume que todas as entradas de log com um determinado [LOG_ID] tenham o mesmo formato. Cada tipo de registro documenta o conteúdo de seu campo de carga útil. Consulte o índice de registros do Stackdriver Logging para exemplos. A seguir estão algumas entradas de log de amostra:

O Compute Engine `syslog` é um tipo de registro personalizado produzido pelo agente de registro `google-fluentd` , que é executado em instâncias de máquina virtual:

```
{
  logName: "projects/my-gcp-project-id/logs/syslog",
  timestamp: "2015-01-13T19:17:01Z",
  resource: {
    type: "gce_instance",
    labels: {
      instance_id: "12345",
      zone: "us-central1-a",
      project_id: "my-gcp-project-id"
    }
  },
  insertId: "abcde12345",
  textPayload: "Jan 13 19:17:01 my-gce-instance
/USR/SBIN/CRON[29980]: (root) CMD (   cd / && run-parts --
report /etc/cron.hourly)"
}
```

Entradas de log de chegada tardia

As entradas de registro exportadas são salvas nos intervalos do Cloud Storage em lotes por hora. Pode levar de 2 a 3 horas para que as primeiras entradas comecem a aparecer. Os fragmentos de arquivos de log exportados com o sufixo `An` ("Anexar") mantêm entradas de log que chegaram atrasadas.

Além disso, o App Engine combina várias `google.appengine.logging.v1.LogLine` subentradas do tipo (também chamadas de AppLog ou AppLogLine) em uma entrada de registro principal do tipo `google.appengine.logging.v1.RequestLog` para a solicitação que causa a atividade de log. Cada uma das linhas de log tem um "ID de solicitação" que identifica a entrada principal. O Logs Viewer exibe as linhas de log com a entrada do log de solicitações. O Stackdriver Logging tenta colocar todas as linhas de registro no lote com a solicitação original, mesmo que seus registros de data e hora o colocassem no próximo lote. Se isso não for possível, a entrada do log de solicitações pode estar faltando algumas linhas de log e pode haver linhas de log "órfãs" sem uma solicitação no próximo lote. Se essa possibilidade for importante para você, esteja preparado para reconectar as partes da solicitação ao processar seus registros.

Integração de terceiros com o Cloud Pub / Sub

O Stackdriver Logging suporta a integração de log com terceiros. Veja Stackdriver Integrations para uma lista atual de integrações.

Você exporta seus registros por meio de um tópico do Cloud Pub / Sub e o terceiro recebe seus registros assinando o mesmo tópico.

Para realizar a integração, espere algo como o seguinte:

1. Obtenha do terceiro um nome de conta de serviço do Google Cloud Platform (GCP) criado a partir do projeto do GCP. Por exemplo, `12345-xyz@developer.gserviceaccount.com` . Você usa esse nome para conceder permissão a terceiros para receber seus registros.
2. Em seu projeto contendo os logs,
3. HABILITA A API
4. Crie um tópico Pub / Sub. Você pode fazer isso quando você configura um coletor de log ou seguindo estas etapas:
5. Vá para a lista de tópicos Pub / Sub .
6. Selecione **Criar tópico** e insira um nome de tópico. Por exemplo, `projects/my-project-id/topics/my-pubsub-topic` . Você exportará seus registros para este tópico.
7. Selecione **Criar** .
8. Autorize o Stackdriver Logging para exportar logs para o tópico. Consulte Definir permissões para o Cloud Pub / Sub .
9. Autorize o terceiro a assinar seu tópico:
10. Fique na lista de tópicos Pub / Sub do seu projeto no Console do GCP.
11. Selecione seu novo tópico.
12. Selecione **Permissões** .
13. Digite o nome da conta de serviço do terceiro.

14. No menu **Selecionar uma função** , selecione **Pub / Sub Subscriber** .
15. Selecione **Adicionar** .
16. Dê a terceiros o nome do seu tópico do Cloud Pub / Sub. Por exemplo, `projects/my-project-number/topics/my-pubsub-topic` . Eles devem se inscrever no tópico antes de começar a exportar.

Comece a exportar os registros quando seu terceiro tiver se inscrito no tópico:

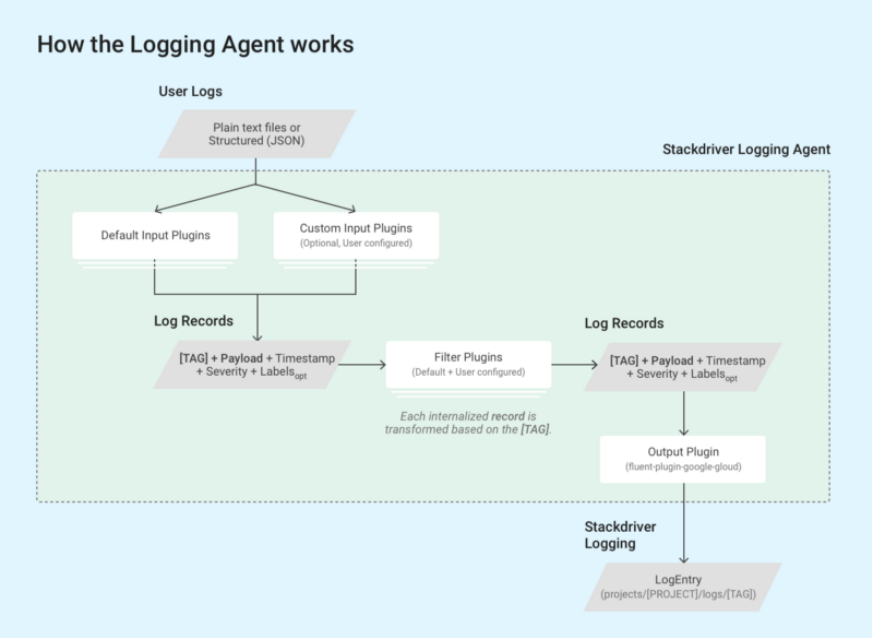
1. Em seu projeto contendo os logs que você deseja exportar, clique em **Criar Exportação** acima da caixa de filtro de pesquisa. Isso abre o painel **Editar exportação** :
2. Digite um **nome de dissipador** .
3. No menu **Serviço de** afundamento, selecione **Cloud Pub / Sub** .
4. No menu **Destino do** Afundamento, selecione o tópico do Cloud Pub / Sub ao qual o terceiro está inscrito.
5. Selecione **Create Sink** para iniciar a exportação.
6. Um diálogo **criado pelo Sink** aparece. Isso indica que seu coletor de exportação foi criado com êxito com permissões para gravar futuros registros correspondentes no destino selecionado.

Seu terceiro deve começar a receber as entradas de log imediatamente.

- -

Sobre o agente de registro

Este guia fornece informações básicas sobre o agente Stackdriver Logging, um aplicativo baseado no fluentd executado em suas instâncias de máquina virtual (VM).



Em sua configuração padrão, o agente do Stackdriver Logging faz o streaming de logs de aplicativos de terceiros e softwares de sistema comuns para o Stackdriver Logging; veja a lista de logs padrão . Você pode configurar o agente para transmitir logs adicionais; Consulte Configurando o agente do Stackdriver Logging para obter detalhes sobre configuração e operação do agente.

É uma prática recomendada executar o agente do Stackdriver Logging em todas as suas instâncias de VM. O agente é executado no Linux e no Windows. Para instalar o agente Stackdriver Logging, consulte Instalando o agente de registro .

Sistemas Operacionais Suportados

Você pode executar o agente Stackdriver Logging nos seguintes sistemas operacionais em instâncias de máquina virtual (VM) compatíveis:

- CentOS 6 e 7
- Debian 7 “Wheezy”, Debian-7-backports, Debian 8 “Jessie” e Debian 9 “Stretch”
- Red Hat Enterprise Linux 6 e 7

- Ubuntu LTS 14.04 "Trusty", 15,04 "Vivid", LTS 16,04 "Xenial", 17,10 "Artful" e LTS 18,04 "Bionic"
- SUSE Linux Enterprise Server 12 SP3, 12 SP2 para SAP e 12 SP3 para SAP
- Windows Server 2008 R2, 2012 R2 e 2016
- Amazon Linux AMI (exceto o Amazon Linux 2.0 AMI)
- Sistema operacional Container-Optimized (suportado apenas para nós do Kubernetes Engine)

Ambientes suportados

O agente do Stackdriver Logging é compatível com os seguintes ambientes:

- Instâncias do Compute Engine . O agente do Stackdriver Logging envia os logs para o projeto associado a cada instância da VM.
- Para instâncias sem endereços IP externos, você deve ativar o Google Private Access para permitir que o agente do Stackdriver Logging envie logs.
- Instâncias do Amazon Web Services Elastic Compute Cloud (AWS EC2) . O agente do Stackdriver Logging envia os logs para o projeto do conector da AWS para o seu espaço de trabalho. O Stackdriver cria este projeto quando você conecta sua conta da AWS a um espaço de trabalho.
- Para que o agente do Stackdriver Logging funcione corretamente, a instância do Amazon EC2 na qual ele é executado deve poder se comunicar com as APIs do Google Cloud, especialmente com a Stackdriver Logging API. Isso requer um endereço IP externo ou um gateway de internet VPC .

Para as instâncias de VM acima, é necessário um mínimo de 250 MiB de memória residente (RSS) para executar o agente do Stackdriver Logging, mas recomenda-se 1 GiB. Por exemplo, a uma taxa de 100 entradas de log de 1 KB por segundo, o agente do Stackdriver Logging com configurações padrão consome 5% da CPU em um núcleo e 150 MB de memória. Com uma taxa de pico de 3.000 entradas de log de 1

KB por segundo, o agente do Stackdriver Logging usa 80% da CPU em um núcleo e 250 MB de memória.

As seguintes instâncias de VMs suportam o Stackdriver Logging usando seu próprio software, possivelmente incluindo versões personalizadas ou configurações do agente Stackdriver Logging. A instalação manual do agente do Stackdriver Logging neles não é suportada:

- Instâncias de VM do ambiente padrão do App Engine . O App Engine inclui suporte integrado para o Stackdriver Logging. Para mais informações, consulte Stackdriver Logging in App Engine Apps .
- Instâncias de VM do ambiente flexível do App Engine . Os aplicativos em execução no ambiente flexível do App Engine podem gravar registros que estão além do que está incluído no ambiente padrão do App Engine. Para mais informações, consulte Stackdriver Logging e o ambiente flexível do App Engine .
- Instâncias do nó do Kubernetes Engine . Você pode ativar o suporte para o Stackdriver Logging nos clusters de contêineres novos ou existentes. Para obter mais informações, consulte Ativação do Stackdriver Logging para o Kubernetes Engine .

Código-fonte do agente do Stackdriver Logging

Você não precisa das informações nesta seção, a menos que queira entender o código-fonte ou tenha outras necessidades especiais. O agente do Stackdriver Logging é instalado pelo script descrito nas instruções de instalação .

O agente do Stackdriver Logging `google-fluentd` , é uma versão modificada do coletor de dados de log fluentd . `google-fluentd` é distribuído em dois pacotes separados. O código fonte está disponível nos repositórios GitHub associados:

- O repositório do GitHub chamado, `google-fluentd` que inclui o `fluentd` programa principal , os scripts de empacotamento personalizado e o plug-in de saída para a Stackdriver Logging API.

- O plugin de saída é empacotado como uma jóia Ruby e está incluído no `google-fluentd` pacote. Ele também está disponível separadamente no serviço de hospedagem gem Ruby no fluent-plugin-google-cloud .
- O repositório do GitHub chamado, `google-fluentd-catch-all-config` que inclui os arquivos de configuração do agente do Stackdriver Logging para a ingestão dos logs de vários pacotes de software de terceiros.

Logs Disponíveis

Esta página fornece informações sobre os registros no Stackdriver Logging e sobre sua estrutura.

Stackdriver Logging recebe, índices, e armazena entradas de log de muitas fontes, incluindo Plataforma Google Cloud, da Amazon Web Services, instâncias VM rodando o Stackdriver Logging agente fluentd , e aplicativos do usuário. Todas as entradas de log no Stackdriver Logging são representadas usando um único tipo de dados `LogEntry` , que define determinados dados comuns para todas as entradas de log, além de transportar cargas úteis individuais. O Stackdriver Logging também pode exportar entradas de registro para o Google Cloud Storage, o Google Cloud Pub / Sub e o Google BigQuery.

O tipo LogEntry

Cada entrada de log no Stackdriver Logging é um objeto do tipo `LogEntry` que é caracterizado pelas seguintes informações:

- O **projeto** ou **organização** que possui a entrada de log.
- O **recurso** ao qual a entrada de log se aplica. Isso consiste em um **tipo** de recurso da Lista de Recursos Monitorados e valores adicionais que denotam uma **instância** específica .
- Um **nome de log** .
- Um **timestamp** .

- Uma **carga útil** , que pode ser um **textPayload** , um **jsonPayload** ou (para serviços do GCP) um **protoPayload** .

Para obter mais informações sobre o conteúdo da entrada de registro, consulte o `LogEntry` tipo na Stackdriver Logging API .

Registros de auditoria

O registro em log do Google Cloud Audit tem três registros:

- Atividade de administração `cloudaudit.googleapis.com/activity` , chamada `activity` no Visualizador de registros
- Acesso a dados `cloudaudit.googleapis.com/data_access` , chamado `data_access` no Visualizador de registros
- Evento do Sistema `cloudaudit.googleapis.com/system_event` , chamado `system_event` no Visualizador de Logs

Os serviços do Google Cloud Platform registram esses registros para ajudar você a responder à pergunta "quem fez o quê, onde e quando?" Em seus projetos do Google Cloud Platform.

A seguir, algumas características das entradas do log de auditoria:

- As entradas de log de auditoria têm o tipo LogEntry , assim como todas as outras entradas de log do Stackdriver Logging.
- Cada entrada de log de auditoria inclui o recurso monitorado ao qual ela se aplica. Você pode encontrar logs de auditoria no menu do seletor de recursos do Visualizador de registros em vários nomes: **BigQuery** , **instância do GCE** , etc.
- A carga útil de cada entrada de log de auditoria é um objeto do tipo `AuditLog` , um buffer de protocolo.
- A carga útil da entrada do log de auditoria possui um campo `serviceData` que alguns serviços usam para reter informações adicionais.
- Todas as entradas do log de auditoria da atividade do administrador são gravadas no log `cloudaudit.googleapis.com/activity` . Cada entrada de log

contém um recurso monitorado que identifica o recurso cuja atividade é auditada.

Logs de auditoria não podem ser excluídos e não estão sujeitos à mesma política de retenção que outros logs. Para mais informações, consulte Log de Auditoria .

Logs de agente

O agente do Stackdriver Logging é um processo baseado no fluentd que pode ser executado em instâncias de VM compatíveis. O agente envia logs do sistema e de terceiros na instância da VM para o Stackdriver Logging, onde eles aparecem como registros separados. Para obter mais informações, consulte Logs do Agente de Registro Padrão .

Registros disponíveis no Stackdriver Logging

Os registros disponíveis no Stackdriver Logging podem variar dependendo de quais recursos do Google Cloud Platform você está usando em seu projeto. Para saber mais, visite a Página inicial da documentação do Google Cloud Platform e selecione o produto ou serviço adequado.

- -

Espaços de trabalho e log do Stackdriver

Você precisa de um espaço de trabalho para enviar logs de uma conta do Amazon Web Service (AWS).

Você não pode usar um espaço de trabalho para visualizar logs de vários projetos e contas da AWS ao mesmo tempo. Você deve visualizar ou exportar os logs de cada projeto e conta da AWS individualmente.

Para obter uma explicação sobre o que são as áreas de trabalho e como elas funcionam, consulte Stackdriver Workspaces . Para obter um guia passo a passo sobre como criar e usar espaços de trabalho, consulte Gerenciando áreas de trabalho .

Acessando Logs da AWS

Para obter registros de uma conta da AWS, siga as instruções para Monitorar uma única conta da AWS ou Monitorar vários projetos . Cada conta da Amazon está conectada ao GCP usando um projeto de conector da AWS . Você encontrará os logs de sua conta da Amazon no projeto do conector, não no Espaço de trabalho que contém as informações de monitoramento.

Você pode descobrir os nomes dos projetos de conector da AWS em uma área de trabalho visitando a página de **configurações** da área de trabalho para a área de trabalho:

IR PARA A PÁGINA DE CONFIGURAÇÕES DA PLATAFORMA DE STACKDRIVER

Acessando logs do GCP de um espaço de trabalho

Se um espaço de trabalho já estiver monitorando vários projetos do GCP, você poderá encontrar as informações de *monitoramento* desses projetos no Espaço de trabalho. No entanto, você deve procurar nos projetos individuais por seus logs - os projetos monitorados ou o projeto de hospedagem no Espaço de Trabalho.

Você pode descobrir quais projetos do GCP estão sendo monitorados por um espaço de trabalho, visitando a página de **configurações** do espaço de trabalho para o espaço de trabalho:

IR PARA A PÁGINA DE CONFIGURAÇÕES DA PLATAFORMA DE STACKDRIVER

. -

Visualizando Logs

Este guia mostra como pesquisar logs e exibir entradas de log com o Visualizador de registros. Para exportar suas entradas de log, consulte Exportando Logs . Para ler as entradas de registro por meio da Stackdriver Logging API, consulte entries.list . Para ler entradas de registro usando o Google Cloud SDK, consulte Lendo entradas de registro .

Começando

1. Vá para a página **Stackdriver> Logging** no console do GCP:
2. Vá para a página do visualizador de registros
3. Selecione um projeto do GCP existente na parte superior da página ou crie um novo projeto.
4. Usando os menus suspensos, selecione o recurso cujos logs você deseja visualizar.

Se você não puder ver nenhum registro, consulte a seção Solução de problemas abaixo.

Espaços de trabalho e registro em log

Você não precisa de um espaço de trabalho para usar o Stackdriver Logging, a menos que queira a capacidade de enviar logs do Amazon Web Services (AWS).

Se você usa o Stackdriver Monitoring e um espaço de trabalho, observe que o Stackdriver Logging não combina logs de projetos monitorados no projeto da conta. Você deve selecionar o projeto cujos logs você deseja ver. Para logs de uma conta do Amazon Web Services, você deve selecionar o projeto do conector do AWS para ver os logs do AWS.

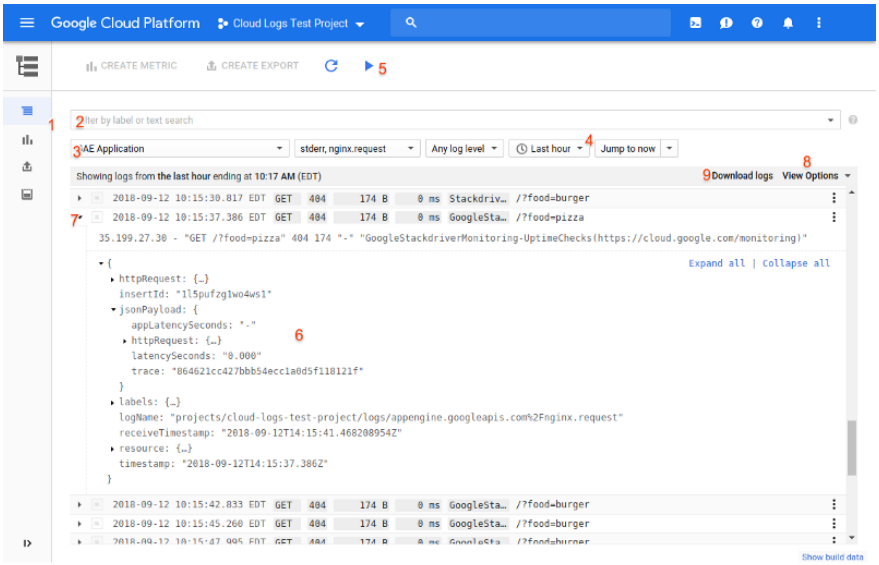
Interfaces de filtro do Visualizador de registros

Existem duas interfaces de filtragem no Visualizador de Registros:

- A interface de filtro básica padrão permite selecionar logs de menus e possui um recurso de pesquisa simples.
- A interface de filtro avançada substitui os menus de interface de filtro básicos por um recurso de pesquisa mais poderoso que você pode usar para exibir entradas de log de vários registros.

Você pode alternar entre as interfaces usando o menu at no lado direito da caixa de filtro de pesquisa em qualquer interface. A captura de tela a seguir mostra o layout do Visualizador de registros. Quatro entradas de

registro das instâncias de VM do Compute Engine são mostradas. A segunda entrada foi expandida clicando na seta de expansão (▸):



A interface de filtro básica possui os seguintes componentes principais - indicados por números vermelhos na captura de tela acima - alguns dos quais são compartilhados com a interface de filtro avançada:

1. As *guias da janela* permitem que você escolha **Logs** , **Métricas** (consulte **Métricas** com base em logs), **Exportações** (consulte Exportando Logs) e **Logs Ingestion** .

2. A *caixa de filtro de pesquisa* na interface de filtro básico permite filtrar entradas de registro por pesquisa de rótulo ou texto. O filtro básico é exibido e o menu no final (▾) alterna para a interface de filtro avançada .

3. Os *menus de seleção básicos* permitem escolher recursos, logs e níveis de severidade para exibição.

4. Os menus suspensos do *seletor de intervalo de tempo* permitem filtrar por datas e horas específicas nos registros.

5. O *seletor de streaming* , na parte superior da página, controla se novas entradas de log são exibidas quando elas chegam.

6. A *tabela de entrada de log* contém as entradas de log disponíveis de acordo com seus filtros atuais e campos personalizados .

7. A *seta de expansão* (►) na frente de cada entrada de registro permite ver o conteúdo completo da entrada. Para mais informações, consulte Expandir entradas de log .

8. O menu **Opções de Visualização** , à extrema direita, possui opções de exibição adicionais.

9. O menu **Download de registros** , na extrema direita, permite baixar um conjunto de entradas de registro. Para detalhes, consulte as entradas do registro de download .

Registros de rolagem e fluxo

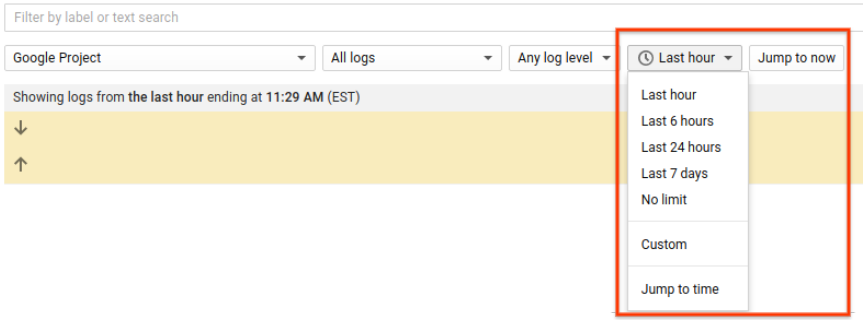
Quando você olha pela primeira vez para o Visualizador de registros, vê entradas de registro recentes suficientes para preencher a tela. Quando você rola através de suas entradas de log, o Visualizador de Logs tenta buscar entradas adicionais. A barra amarela acima e abaixo dos registros permite saber se mais entradas de log podem estar disponíveis. Usando o menu **Opções de Visualização** , você pode selecionar a ordem na qual exibir as entradas de registro.

Ícones na parte superior do controle de tela quando os logs são atualizados:

- O ícone “atualizar” (“Ir para os registros mais recentes”) recuperará os registros mais recentes e rolará a exibição para eles.
- O ícone “play” (▶) começará a transmitir os logs mais recentes. Ele pára se você selecionar uma entrada de registro ou rolar a exibição de registros.
- O ícone de “pausa” (pa) interromperá a transmissão dos registros mais recentes.

Vá até uma hora

Você pode filtrar suas entradas de registro por hora e data usando os menus do *seletor de intervalo de tempo* abaixo da caixa do filtro de pesquisa.

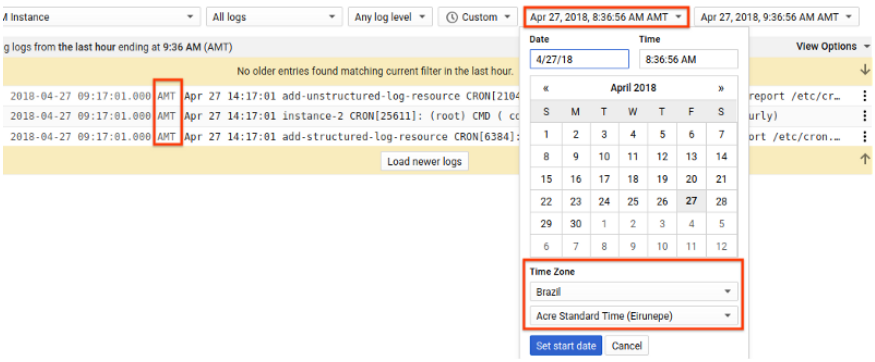


A seleção padrão é **Última hora** . Você pode usar o menu suspenso para selecionar outros intervalos de tempo ou definir um intervalo **personalizado** . Selecione **Saltar para a hora** para filtrar os registros para uma data e hora específicas ou use o menu **Ir para agora** para ver as entradas de registro atuais. Depois de ter feito a sua seleção, você pode rolar os logs para inspecionar as entradas em torno desse tempo. Clicar nos ícones **Atualizar** ou **Reproduzir** na parte superior da página redefinirá a data e a hora nesse menu para a entrada de registro recebida mais recentemente.

Alterar o fuso horário

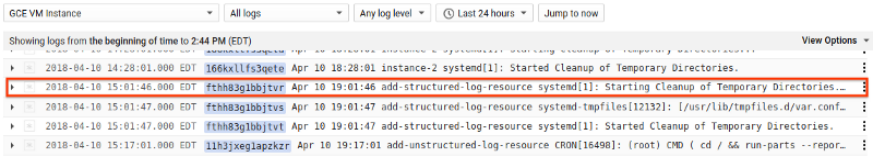
Você pode selecionar um fuso horário para filtrar seus registros:

1. Conforme mostrado na captura de tela anterior do menu suspenso, em **Última hora** , selecione **Personalizar** . Dois novos menus suspensos aparecem à direita de **Personalizar** .
2. Clique na seta do expansor (▾) em qualquer um dos novos menus. Um menu de calendário suspenso é exibido.
3. Na seção **Fuso horário** do menu de calendário, selecione seu país e fuso horário preferidos.
4. Seu Visualizador de registros exibe sua preferência de fuso horário atualizada:



Expandir entradas de log

A tabela de entrada de log exibe uma linha de resumo para cada entrada de log por padrão. A seguir, uma captura de tela com uma linha de resumo destacada em vermelho:



O Visualizador de registros destaca certos campos da entrada de registro na linha de resumo. Certos campos são exibidos por padrão se atenderem a esses critérios:

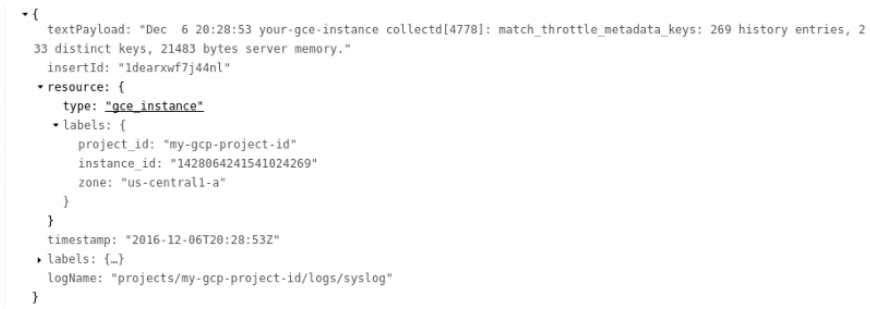
- A entrada de registro tem um tipo conhecido, como um log de solicitações do App Engine.
- Caso contrário, quando a entrada de log contiver o `httpRequest` campo.
- Caso contrário, quando a entrada de log tiver uma carga útil contendo um campo denominado `message` .

Você também pode adicionar outros campos à linha de resumo; consulte Adicionar campos personalizados para detalhes.

Para ver os detalhes completos de uma entrada de registro, clique na seta de expansão (▸) na frente da linha de resumo. Para ver os detalhes completos em uma visualização estruturada de todas as entradas de registro disponíveis com o filtro atual, clique no menu **Opções de visualização** na extrema direita e selecione **Expandir tudo** :

Você pode selecionar **Recolher tudo** para recolher todos os detalhes da entrada do log expandido.

Ao expandir uma linha de resumo para uma entrada de log, você verá uma visualização estruturada (JSON) para essa entrada de log:



Para obter uma descrição dos campos na entrada, consulte o tipo LogEntry .

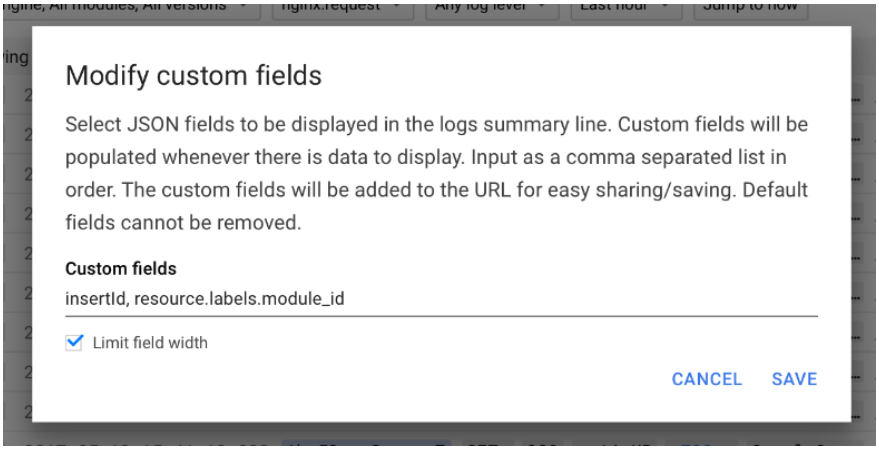
Adicione campos personalizados

Campos personalizados são campos dentro de entradas de log que você pode trazer para uma linha de resumo para o resumo da entrada de log principal.

Existem duas maneiras de adicionar campos personalizados às linhas de resumo da tabela de entrada de log:

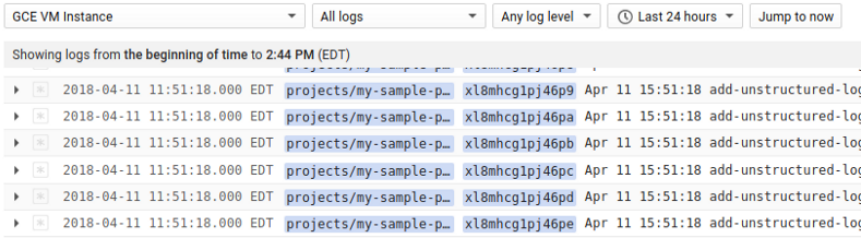
- Em uma entrada de log expandida , clique em um campo dentro da representação JSON. No painel resultante, selecione **Adicionar campo à linha de resumo** :

- No menu **Opções de Visualização,** na parte superior direita do Visualizador de Registros, selecione **Adicionar campos personalizados** (se você tiver campos personalizados existentes neste projeto, esta opção será **Modificar campos personalizados**). No painel resultante, adicione a chave JSON desejada e clique em **Salvar** . Você pode adicionar várias chaves separando-as com uma vírgula. Para reorganizar a aparência de seus campos personalizados em suas linhas de resumo, reorganize o texto neste painel e clique em **Salvar** .



Campos personalizados são preenchidos sempre que estiverem disponíveis nas entradas de log. Os campos personalizados são adicionados ao seu URL atual e permanecem enquanto você estiver usando esse URL ou estiver na mesma sessão do navegador. Você não pode defini-los em um nível global e eles não podem ser salvos por usuário ou por projeto do GCP.

Campos personalizados são destacados em azul na sua tabela de entrada de log:



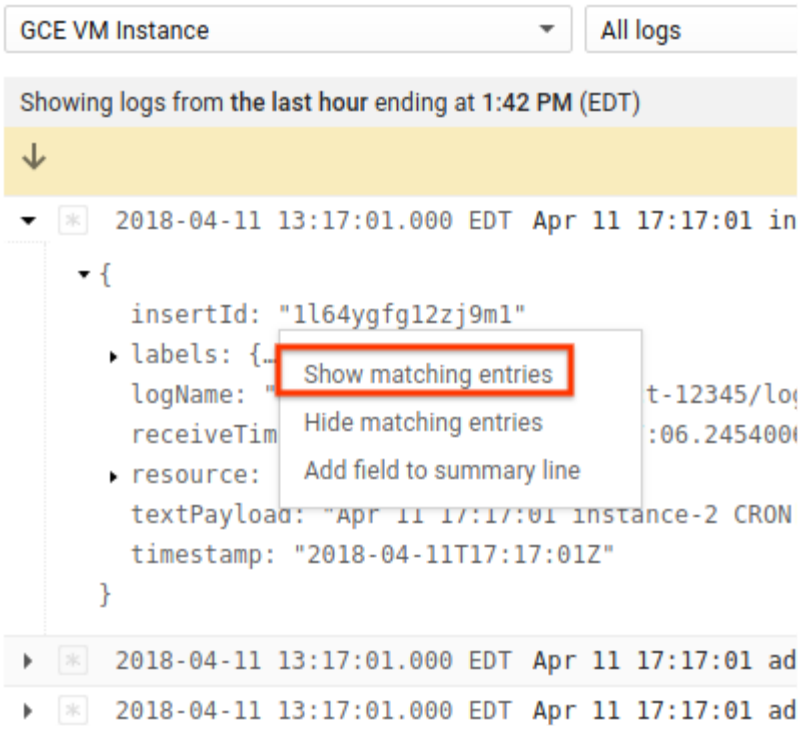
Existem duas maneiras de remover campos personalizados das linhas de resumo da tabela de entrada de log:

- Em qualquer linha de resumo que contenha o campo personalizado que você deseja remover, clique no campo e selecione **Remover campo da linha de resumo** .
- No menu **Opções de visualização,** na parte superior direita do Visualizador de registros, selecione **Modificar campos personalizados** . No painel resultante, exclua as chaves JSON que você deseja remover e clique em **Salvar** .

Campos padrão não podem ser removidos da tabela de entrada de log.

Mostrar registros semelhantes

Você pode clicar no valor de um campo individual na exibição de entrada de log expandida e, em seguida, mostrar ou ocultar todas as entradas de log com o mesmo valor:



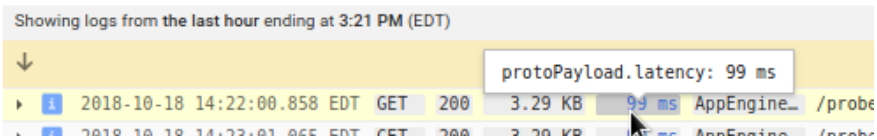
Quando você faz isso, o Visualizador de registros é alterado para a interface de filtro avançada. Para modificar a pesquisa, edite o filtro e clique em **Enviar filtro** . Para mais informações, consulte a interface avançada do filtro .

Além disso, você pode correlacionar as entradas do log de solicitações do App Engine e visualizá-las em uma estrutura aninhada. Para obter detalhes, consulte Exibindo entradas de log de solicitações relacionadas e selecione seu idioma de tempo de execução.

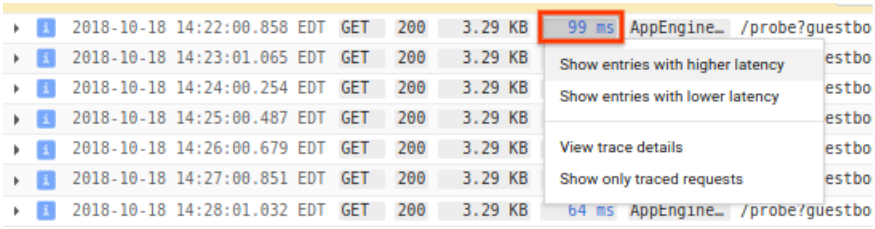
Mostrar detalhes da latência

Novo! Para os **logs de solicitação do Google App Engine** , o Visualizador de registros fornece um link para o Stackdriver Trace para facilitar a visualização dos detalhes de latência da entrada de registro.

Para mostrar o menu de opções relacionadas à latência para uma entrada de log, identifique o `protoPayload.latency` campo:



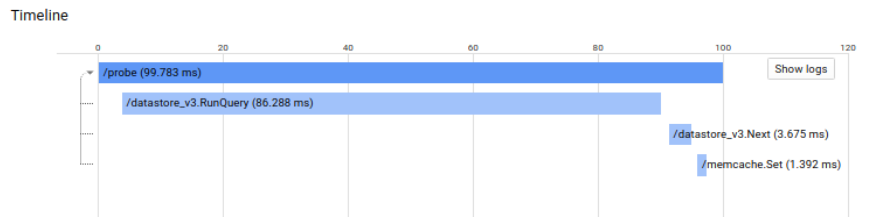
Clique no valor de latência:



As duas primeiras opções no menu restringem as entradas de log mostradas àquelas com latências maiores ou menores. A última opção no menu restringe as entradas de log àquelas que contêm detalhes de rastreamento visíveis pelo Stackdriver Trace. Especificamente, a última opção restringe as entradas de log àquelas em que **os detalhes do rastreio do View** estão ativados.

Visualizar detalhes da latência no Stackdriver Trace

Para determinados registros de solicitações do App Engine, a opção **Visualizar detalhes de rastreamento** está ativada. Quando ativado, clique nessa opção para abrir o Stackdriver Trace e exibir os detalhes de latência da entrada do registro:



Selecionando logs

Use os menus e a caixa de filtro para encontrar os registros que você deseja ver:

- **Selecione um tipo de recurso e uma instância** cujos logs você deseja ver. Você pode examinar todas as instâncias desse tipo de recurso ou selecionar uma instância específica. Na captura de tela acima, a **instância da VM G C E** (todas as instâncias) está selecionada. Para obter uma lista de tipos de recursos, consulte Lista de recursos monitorados .

- **Selecione os logs nomeados que** você deseja ver no segundo menu ou selecione **Todos os registros** . O menu mostra os logs que estão em uso pelas instâncias de recursos selecionadas.
- **Selecione o nível de gravidade mais baixo que** você deseja ver no terceiro menu. Selecionar **Qualquer nível de log** também mostrará entradas de log que não possuem gravidade atribuída.
- **Selecione o intervalo de tempo que** você deseja ver no quarto menu ou selecione **Ir para agora** no quinto menu.

À medida que você altera suas seleções de menu, você verá as entradas de log correspondentes.

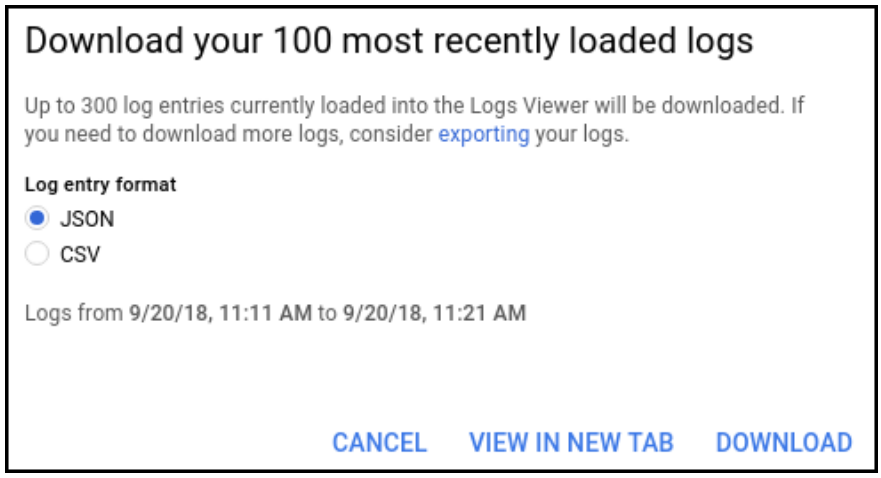
Notas do menu :

- Apenas os tipos de recursos, instâncias e nomes de log que estão presentes em seu projeto são mostrados nos menus. Pode demorar um pouco para os menus serem atualizados após adicionar um novo tipo de recurso ou instância, ou gravar em um novo log.
- Na interface de filtro básica, você pode examinar apenas as entradas de log de um tipo de recurso de cada vez. A interface de filtro avançada permite vários tipos de recursos.
- Você não verá nenhum registro se navegar até uma hora anterior à sua janela de retenção atual. Para mais informações, consulte os períodos de retenção Logs .

Download de entradas de log

Com alguns cliques, você pode baixar, no formato JSON ou CSV, todas as entradas de log armazenadas na memória de trabalho do Visualizador de registros. Por motivos de desempenho, o Visualizador de registros tenta carregar 100 entradas de registro de cada vez e não retém mais do que 300 entradas de registro em sua memória de trabalho. Esses valores não são configuráveis.

Para fazer o download de entradas de registro, clique no menu **Download de registros** , localizado na parte superior direita do Visualizador de registros. Na caixa de diálogo de download, selecione JSON ou CSV para o **formato de entrada de log** e clique em **Download** :



Para exibir entradas de log formatadas em JSON ou CSV em uma página da Web, siga as mesmas etapas que para um download, mas selecione **Exibir em nova guia** .

Pesquisando com o Visualizador de Logs

Você pode restringir ainda mais suas pesquisas usando filtros nas interfaces de filtro básica e avançada. A interface de filtro avançada contém a maioria dos recursos da interface de filtro básica, mas permite recursos de pesquisa mais eficientes.

Para obter mais informações sobre como pesquisar com a interface de filtro básica, consulte Filtros de Logs Básicos . Para mais informações sobre pesquisas avançadas, consulte Filtros de Logs Avançados .

Diferenças entre filtros básicos e avançados

Se você estiver familiarizado com as pesquisas de texto e de campo da interface de filtro básica, aqui estão algumas dicas para ajudá-lo com os filtros de logs avançados.

Não use "texto:"

O Visualizador de registros mostra pesquisas de texto no filtro básico, prefixando o texto com o rótulo `text:` . O `text:` rótulo não deve ser usado com filtros avançados. A tabela a seguir mostra pesquisas de texto equivalentes:

Filtro básico do Visualizador de registros Filtro de registros avançados com o mesmo significado `text:"one two""one two"text:threethreetext:n=5"n=5"` (aspas são necessárias)

Se você acidentalmente usar `text:` o filtro avançado, estará procurando uma correspondência em um campo chamado `text`, que não existe.

Verifique os nomes dos campos

A interface de filtro básica possui nomes de campo internos para determinados registros, incluindo o log de solicitações do App Engine. Esses nomes de campo não existem em filtros avançados. Por exemplo, a tabela a seguir mostra uma pesquisa de campo equivalente para um log de solicitações do App Engine:

Filtro básicoFiltro avançado `querystring:var=3protoPayload.resource:"var=3"status:400..405protoPayload.status >= 400 AND protoPayload.status <= 405`

Se a primeira amostra, se você acidentalmente usar o nome do campo de filtro básico, você estará procurando por um campo chamado `querystring`, que não existe, então o Visualizador de Logs não encontrará nenhum log.

Jogos de subcadeia

Na interface de filtro básica, todas as pesquisas são correspondências de substring sem distinção entre maiúsculas e minúsculas. Ou seja, as pesquisas `text:abc` ou `somefieldname:abc` irá corresponder entradas contendo log `abc`, `xyabcyx` e `ABc`. Nos filtros de log avançados, você deve usar o operador de pesquisa "has" (`:`) para o mesmo comportamento.

Para uma correspondência exata, use o operador equals (`=`). A comparação `field=abc` requer que `field` contenha exatamente `abc`, em qualquer caso de letra. Essa pesquisa não pode ser expressa na interface básica do filtro.

AND e OR

Na interface de filtro básica, duas comparações usando o mesmo nome de campo (ou `text:`) são implicitamente associadas `OR`, enquanto comparações com rótulos diferentes são unidas `AND`. Nos filtros de logs avançados, todas as comparações são unidas, a `AND` menos que `OR` seja especificado explicitamente. Você também pode usar parênteses para agrupar comparações. A tabela a seguir mostra pesquisas equivalentes nas duas interfaces de filtro:

Pesquisa básica de filtrosPesquisa avançada de filtros `text:abc` `querystring:def text:xyzprotoPayload.resource:"def" AND ("abc" OR "xyz")`

Desempenho de pesquisa

Veja algumas dicas para aumentar seu desempenho de pesquisa:

- Pesquise valores específicos de campos indexados, como o nome da entrada de log, o tipo de recurso e os rótulos de recursos. Na interface de filtro básica, você faz isso com seleções de menu. Na interface de filtro avançada, use condições como as seguintes:

- `resource.type = "gce_instance"` `logName = "project/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Factivity"` `resource.labels.module_id="default"` `resource.labels.instance_id="1234567890`

- Escolha correspondências exatas em pesquisas de substring. Especialmente nos campos de índice, as correspondências parciais são mais lentas. Na interface de filtro básica, todas as pesquisas de texto são correspondências parciais. Na interface de filtro avançada, favor testar usando o operador de igualdade (`=`) em vez de usar "has" (`:`).

- Encurte o período de tempo pesquisado. Você não pode fazer isso na interface de filtro básica, mas na interface de filtro avançada você pode especificar um intervalo de tempo:

- `timestamp >= "2016-11-29T23:00:00Z" AND timestamp <= "2016-11-29T23:30:00Z"`

Para obter mais informações sobre desempenho, consulte Localizando entradas de log rapidamente .

Solução de problemas

Esta seção fornece instruções para solucionar problemas comuns encontrados ao interagir ou pesquisar com o Visualizador de registros.

Não há registros!

Se você não vir nenhum registro, verifique o seguinte:

- **O projeto correto está selecionado no topo da página?** Caso contrário, use o menu suspenso na parte superior da página para selecionar um projeto. Você deve selecionar o projeto cujos logs você deseja ver.
- **Seu projeto tem alguma atividade?** Mesmo que o projeto seja novo, ele deve ter logs de atividade ou auditoria registrando o fato de que ele foi criado. Você pode obter mais registros indo até o início rápido .
- **O intervalo de tempo é muito estreito?** Você pode usar os menus suspensos abaixo da caixa do filtro de pesquisa para selecionar outros intervalos de tempo ou definir um intervalo **personalizado** . Selecione **Saltar para a hora** para filtrar os registros para uma data e hora específicas ou use o menu **Ir para agora** para ver as entradas de registro atuais.

Minha pesquisa não está funcionando!

Se você não tiver certeza de por que sua pesquisa não está funcionando na interface básica do filtro, alterne rapidamente para a interface de filtro avançada:

1. Selecione **Converter para filtro avançado** no menu at no final da caixa de pesquisa.
2. Olhe para o filtro avançado para ver se é o que você pretendia.
3. Volte para a interface de filtro básica usando o botão **Voltar** do navegador .

Aqui estão algumas outras razões pelas quais você pode não ver todas as entradas de log esperadas:

- Não é possível ver entradas de registro mais antigas que o período de retenção do Stackdriver Logging. Consulte Política de cotas para o período de retenção de registros em vigor.
- Durante períodos de carga pesada, pode haver atrasos no envio de registros para o Stackdriver Log ou no recebimento e exibição dos registros.
- O Visualizador de registros não mostra as entradas de registro que possuem registros de data e hora no futuro, até que a hora atual seja "capturada". Essa é uma situação incomum, provavelmente causada por uma distorção de tempo no aplicativo que envia os logs.

- -