Audit Logging

This page describes how to use audit logging with VPC Service Controls.

Note: For more information on finding VPC Service Controls errors using Stackdriver Logging, refer to the Troubleshooting (https://cloud.google.com/vpc-service-controls/docs/troubleshooting#vpc-sc-errors) page.

VPC Service Controls logs all accesses that are denied because of security policy violations to Stackdriver Logging by default. The audit log records are securely stored in Google infrastructure and available for future analysis. Each generated record is intended for one recipient. Only this recipient has access to the record and it is not visible to any other entity. A recipient can be a project, a folder or an organization.

The content of the audit log is available on a per project basis in the Google Cloud Console. The VPC Service Controls audit log is written into the "Audited Resource" logging stream and is available in Stackdriver Logging.

Note: Cloud Storage data access logging needs to be enabled in order to enable VPC Service Controls audit logging.

Generating the audit log record

Each request that is denied due to violation of security policy can result in more than one auditing record. These generated records will be identical but will address different recipients. Generally each request contains a number of resource URLs. Each such resource has an owner (where the owner can be a project, folder or organization). The VPC Service Control API will

determine owners for each resource participating in the failing request and generate a record for each.

Audit log record content

Each audit log record contains information which can be divided into two major categories: the information about the original call, and information about security policy violations. It is filled by VPC Service Controls API as follows:

Audit Log Field	Meaning
`service_name`	The name of the service handling the call that resulted in the creation of this audit record.
`method_name`	The name of the method call that resulted in the security policy violation described in this record.
`authentication_info.principal_email`	Email address of the user issuing the original call.
`resource_name`	Intended recipient of this audit record (can be a project, a folder or an organization).
`request_metadata.caller_ip`	The IP address from which the call originated.
`request_metadata.caller_is_gce_client`	True if the original call was made from a Compute Engine network. False otherwise.
`request_metadata.caller_gce_network_project_number`	Project number corresponding to Compute Engine network from which the original call was made, if the call was made from a Compute Engine network.
`request_metadata.caller_internal_gce_vnid`	Internal VNID of Compute Engine caller if the call was made from a Compute Engine network.
`status`	The overall status of handling an operation described in this record.
`metadata`	An instance of `google.cloud.audit.`

	`VpcServiceControlAuditMetadata` protobuf type, serialized as a JSON Struct. Its 'resource_names' field will contain a list of all resource URLs participating in the failed VPC Service Controls policy check.

Accessing the audit log

The content of the audit log is available on a per project basis in the Google Cloud Console. The VPC Service Controls audit log is written into the “Audited Resource” logging stream and is available in Stackdriver Logging.

Last updated December 4, 2019.