Google Cloud 故障事件2020.1-2024.10

Google Cloud Service Health: (https://status.cloud.google.com/summary) 时长>10h，且具有完整报告的

故障大类型分为：电力故障、系统硬件故障、系统软件错误、网络故障

序号	事件时间	影响时长	事件描述	故障分析	故障在系统中的表现	故障归因
1	12 Jun 2024 Incident began at **2024-06-12 12:06** and ended at **2024-06-12 15:59**	3 hours, 53 minutes	2024 年 6 月 12 日（星期三）美国/太平洋时间 12:06，Google Vertex AI、Dialogflow、Agent Assist 用户在美国中部 1 区、亚洲东南部 1 区、欧洲西部 3 区、欧洲西部 4 区、美国东部 1 区、美国西部 1 区、北美东北部 1 区和美国东部 4 区遇到错误和产品功能问题，持续时间为 3 小时 53 分钟。	根本原因 从 2024 年 6 月 8 日开始，用户对 GenerateContent API 的一种新型请求引发了顶点服务预测 API 服务器的间歇性分段故障。 受影响的服务器会在分段故障后重新启动，负载平衡器会将用户查询发送到其他健康的 API 服务器，直到受影响的服务器恢复服务。 当触发故障的流量增加，且同时离线的 API 服务器数量足以影响整体服务能力（相对于负载而言）时，用户可见的中断就开始了。		**软件错误导致服务失效** （API服务设计缺陷）
2	2024-3-20 Incident began at **2024-03-20 09:58** and ended at **2024-03-20 14:45**	4 hours, 47 minutes	Dialogflow ES、Dialogflow CX、Cloud Speech-to-Text 和 Agent Assist 在两个时段分别出现了 1 小时 42 分钟和 30 分钟的流数据平面流量错误升高。 根据初步分析，问题的根本原因是最近对作为受影响产品后端网关的内部关键依赖项进行了配置更改。	2024 年 3 月 20 日，美国/太平洋时间 11:40，谷歌工程师撤销了对内部关键依赖关系的配置更改，从而在制定永久解决方案时暂时缓解了影响。 美国/太平洋时间 14:15，依赖关系服务完成了先前计划的推出，无意中撤销了工程师实施的临时缓解措施。 2024 年 3 月 21 日，美国太平洋时间 16:31，工程师有效实施了包含必要缓解措施的新版依赖性服务，成功防止了任何进一步的回归。		**软件错误导致服务降效** （配置错误）→（错误率升高）
3	2024-3-30 Incident began at **2023-03-30 04:04** and ended at **2023-03-30 20:28**	8 hours, 43 minutes	摘要：我们正在调查针对 PostgreSQL 的 AlloyDB 问题： 截至 2023 年 3 月 30 日（星期四）美国太平洋时间 07:10，工程师已经缓解了从还原中创建的新集群的问题。 大多数客户的问题应该可以恢复，但工程部正在采取额外的步骤，以确保所有受影响的客户完全恢复，这项工作尚未确定全面完成的 ETA。 我们将继续提供有关任何更改的更新，并将在 2023 年 3 月 30 日（星期四）美国太平洋时间 21:30 之前提供更多信息。 诊断： 客户在尝试在已恢复的群集中创建主实例时会遇到此问题。 客户在尝试创建实例时会看到内部错误（错误代码：13）。 解决方法： 客户可以从同一备份重新恢复，并可能删除已损坏的旧备份。			**软件错误导致服务失效**
4	2023-4-25 Incident began at **2023-04-25 16:46** and ended at **2023-04-26 20:00**	1 day, 3 hours	Europe-west9 包含三栋建筑，具有独立的冷却、供电和网络。区域 Spanner 支持该区域大多数 Google 云服务的区域控制平面。在 europe-west9 中，区域 Spanner 的副本没有正确地分布在该区域的三座建筑中，以确保受影响建筑断电后的法定人数可用。因此，europe-west9 中许多 Google 云服务的控制平面服务中断，导致该地区的这些服务不可用和/或错误率升高。Regional Spanner 已于 2023 年 4 月 26 日 12:47 美国/太平洋时间恢复。 包括 Cloud Console 在内的 Google 云服务都依赖于这些方法。当 europe-west9 区域和分区的 GCE 控制平面离线时，其中一些扇出方法无法正常运行。在断电期间，这导致 Cloud Console 中的某些页面和控制平面操作在全球范围内不可用。	水泄漏和火灾损失 2023 年 4 月 25 日（星期二）美国/太平洋时间 16:46，欧洲-西方 9 区的一个数据中心发生冷却系统水管泄漏。 泄漏源于设施的非谷歌部分，进入相关的不间断电源 (UPS) 机房，并导致火灾。 火灾发生后，当地消防部门需要疏散设施人员，并将整个数据中心大楼的电源关闭数小时。 大火于 2023 年 4 月 26 日美国/太平洋时间 04:11 被成功控制。		**硬件故障导致服务失效** （火灾导致数据中心设备关闭）→（服务失效）

5	2023-11-21 Incident began at **2023-11-21 07:43** and ended at **2023-11-21 15:33**	7 hours, 51 minutes	摘要：当映像 URL 被 Kubernetes-digester 覆盖时，MDP（istio 组件）会持续驱逐 pod，istio 版本为：1.14.6-asm.23 和 1.14.6-asm.24 描述：从 2023-11-21 06:39 美国太平洋时间星期二开始，我们遇到了 Anthos Service Mesh 问题	诊断：当代理镜像 URL 被 Kubernetes-digester 覆盖时，客户可能会遇到其 Anthos Service Mesh (ASM) pod 被持续（有时是同时）驱逐的情况。		**软件错误导致服务失效**
6	022-5-6 Incident began at **2022-05-06 01:30** and ended at **2022-05-06 12:06**	10 hours, 36 minutes	2022 年 5 月 6 日美国/太平洋时间 01:30，多个 Google 云服务在 us-central1 区域出现问题。 这些问题主要集中在 us-central1-b 区域服务，但也有一些区域服务出现性能下降，直到其流量从受影响区域转移出来。 在根本问题得到解决后，大多数 Google 云服务都能自动恢复。	谷歌云系统建立在一个名为 Colossus 的分区分布式存储系统之上，该系统在大量名为 D 服务器的独立存储服务器之间复制数据。在此次事件中，负责重新打包存储对象的后台作业开始更积极地重试这些重新打包操作，将其作为正常操作的一部分。这增加了该区域 Colossus 系统的负载，包括与 D 服务器的开放连接数量。 D 服务器的连接负荷突然增加，导致少数服务器因内存压力过大而意外崩溃。这导致我们的自动管理系统将它们从 Colossus 服务机群中移除。这进一步减少了可用于处理不断上升的流量负载的D服务器数量，并增加了受影响区域内Colossus系统的流量延迟。	延迟的显著增加影响了我们客户在Colossus之上构建的一系列谷歌云服务的性能，包括持久磁盘、BigQuery等。 由于特定的故障模式，该区域事件影响了一些区域服务。当Colossus集群被标记为宕机时，区域服务会收到主动通知，并自动将流量从集群中转移出来。由于该群集仍在运行，但某些操作的延迟不稳定，区域服务没有收到主动通知，也无法自动将流量从群集转移走。因此，对一些区域服务的影响扩大了，因为它们必须手动将受影响的群集从服务中移除。	**硬件故障导致服务降效** （服务器内存使用率超限）→ (服务降效)
7	2024-2-28 Incident began at **2024-02-28 23:50** and ended at **2024-02-29 09:50.**	10 hours	Chronicle Security SIEM 和 Chronicle SOAR 在美国/多地区的 Backstory API 调用中出现远程过程调用 (RPC) 错误率升高，持续时间共计 10 小时。 我们的工程师确定了部分根本原因进程，并在 2024 年 2 月 29 日（星期四）美国/太平洋 06:18 时消除了这些进程。 但是，在最初的分析中遗漏了其中一些流程，导致 7:13 时出现额外的流量和资源争用。 工程师们采取了更多措施，进一步缓解了 09:50 时的问题。			**软件错误导致服务降效** （API调用错误）→ (资源争用)
8	2024-1-23 Incident began at **2024-01-23 09:30** and ended at **2024-01-24 22:00**	1 day, 13 hours	2024年1月23日（周二）上午09:30 PT，Google Cloud的Cloud Logging及依赖于Cloud Logging的其他产品和服务在多个区域（包括us-central1、us-east1、europe-west1、europe-north1、asia-east1）发生了日志处理延迟。受影响的时间窗口如下： • **us-central1**: 09:30 - 13:30 PT，约4小时 • **us-east1**: 09:30 - 10:20 PT，约50分钟 • **europe-west1**: 09:30 - 14:15 PT，约4小时45分钟 • **europe-north1**: 09:30 - 14:15 PT，约4小时45分钟 • **asia-east1**: 09:30 - 10:10 PT，约40分钟 在此期间，用户无法通过Google Cloud控制台或API查询日志，日志的导出和基于日志的指标写入也出现延迟。此外，个性化服务健康（PSH）的警报也受到了影响，但所有日志最终都成功处理和存储，没有发生日志丢失。	此次故障的根本原因在于Cloud Logging中的动态资源分配机制。当某些日志桶启用了日志分析（Log Analytics）功能时，系统需要为这些日志动态分配存储资源，并更新配置数据库的状态。这些配置是日志摄取和路由过程中的关键环节，确保数据能够按照客户组织的要求进行存储和处理。 在此次事件中，工程团队为新的项目组增加了日志分析功能，导致多个区域内同时发出大量动态资源分配请求，进而造成配置数据库访问竞争和处理速度减慢。虽然日志路由器具备负载削减机制以防止吞吐量下降，但由于一个未知的问题，该机制未能及时隔离问题流量，导致日志路由器的吞吐量在受影响区域降低约40%，最终引发日志处理积压。 为了应对积压问题，Google工程团队扩展了日志分析和基于日志的指标处理管道。然而，此次扩展又引发了两个次要问题： 1. **基于日志的指标查询性能下降**：由于数据的高基数，部分用户的查询在事件发生后的25小时内出现超时问题。 2. **日志分析（Log Analytics）查询失败**：由于扩展导致超过了内部连接配额，导致在事件期间日志分析查询无法返回最新的日志数据。		**软件错误导致服务降效** （动态资源佩芬机制错误）→ (网络流量增高，区域服务降效)
9	2024-3-24 Incident began at **2024-03-24 02:59** and ended at **2024-03-24 11:07**	8 hours, 8 minutes	2024年3月24日（星期日）02:59 PT，Google的Contact Center AI (CCAI) 平台出现问题，导致部分或全部实例不可用。受影响期间，客户在尝试联系呼叫中心时会收到"应用程序错误"，且无法被重定向到IVR（交互式语音应答系统）。此外，当用户尝试登录CCAI时，会被默认设置为“离线状态”，并无法使用平台功能。	数据库连接错误导致多个实例不可用 在故障发生时，客户尝试与呼叫中心进行联系时，由于未能正常与IVR系统连接，导致应用程序报错。登录CCAI平台的用户无法在线，系统默认将其状态设置为离线，平台的功能也无法正常使用。		**软件错误导致服务失效** （数据库连接错误）→ (众多服务失效)

10	2023-12-6 Incident began at **2023-12-06 04:20** and ended at **2023-12-06 16:47**	12 hours, 27 minutes	2023年12月6日04:20（美国太平洋时间），Google App Engine Flex 服务在多个区域发生应用不可用问题，持续时间为12小时27分钟。受影响的区域包括多个亚太、欧洲、美洲区域，如asia-east1、europe-west1、us-central1等。 此次故障是由于无效的后端服务配置更新，导致L7负载均衡器（Layer 7 Load Balancer）在多个区域的状态不一致。问题在12月6日16:47通过回滚配置变更得以解决。	事件的根本原因是一项无效的后端服务配置更新。这项错误的配置导致L7负载均衡器的状态在不同区域出现不一致，进而引发了应用不可用的问题。L7负载均衡器负责将客户端请求分发到后端服务，但由于状态不一致，负载均衡器无法正确选择后端服务器，导致HTTP请求返回502错误（Bad Gateway）。 问题产生后，用户的Google App Engine Flex应用可能在部署过程中显示成功，但在运行一段时间后变得不可用。受影响的用户会遇到"failed_to_pick_backend"的错误消息。		**软件错误导致服务失效** (配置错误) → （服务失效）
11	2023-11-20 Incident began at **2023-11-20 20:00** and ended at **2023-11-21 05:50**	9 hours, 50 minutes	2023年11月20日，Google BigQuery的后台容量管理系统在EU多区域（EU multi-region）发生问题，持续时间为9小时50分钟。在此期间，BigQuery客户无法购买新的计算槽位（slots），并且自动扩容功能（autoscaler）无法正常工作。这影响了使用BigQuery自动扩展功能的客户，导致他们无法在负载增加时自动扩展资源。	BigQuery的容量管理系统负责批准槽位请求，并根据当前的客户位置、容量及预订大小，从内部数据库中获取信息，来确定可用的容量。 此次故障的根本原因是容量管理服务中的一个问题，导致无效的数据条目写入了该数据库。由于这个无效条目，系统错误地显示区域内没有可用的槽位容量。因此，客户无法在EU多区域购买新的槽位，也无法进行自动扩容。		**软件错误导致服务失效** （容量管理服务错误） → （容量扩展服务失效）
12	2024-4-16 Incident began at **2024-04-16 02:20** and ended at **2024-04-17 03:40**	1 day, 1 hour	2024年4月16日至17日期间，Cloud Composer的部分用户在使用“Private IP”配置创建、调整大小或升级到Cloud Composer 2的新版本时，遇到了高失败率，持续时间为1天1小时20分钟。在此期间，已有的“Private IP”环境如果未进行升级或调整大小则运行正常。 受影响用户主要是尝试创建、升级或调整Cloud Composer环境的用户，其中约有少于200个客户项目创建失败，少于20个环境因升级失败受影响。	此次故障的根本原因是由于Cloud Composer使用的最新稳定版容器操作系统（COS）镜像中的变更导致的。最新的COS镜像（M113版本）将默认防火墙规则管理工具从iptables-legacy切换为iptables-nft，这个变化影响了负责执行容器的系统组件Konlet，使其在处理iptables规则时出现问题，从而导致创建、升级和调整操作失败。		**软件错误导致服务失效** （配置错误） → (失败率升高)
13	2024-1-10 Incident began at **2024-01-10 07:23** and ended at **2024-01-12 03:08**	1 day, 20 hours	2024年1月9日08:30 PST至2024年1月10日16:45 PST，Google Cloud Monitoring和所有依赖该监控服务的Google Cloud产品发生了数据延迟、指标查询失败及服务指标数据不可用的情况。此问题持续了1天19小时45分钟，且在1月10日09:30 PST至16:45 PST期间影响尤为严重，持续了7小时15分钟。问题源于两个不同的故障：**指标数据查询延迟**和**指标数据不可用**。	1. **指标数据查询延迟**： • 数据从内存到磁盘的存储过程发生了瓶颈。2024年1月9日08:30 PST，一项关于us-central1区域数据复制的配置变更引发了处理数据的管道阻塞，导致积压。这一问题最初并未对用户可见，因为最近24小时的数据仍然能够通过内存层提供。 • 1月10日08:00 PST，该管道问题得到缓解，但积压的20小时数据迅速被写入磁盘查询系统，导致文件激增，进一步引发了另一个磁盘系统瓶颈，导致大部分查询出现高延迟或失败。 2. **指标数据不可用**： • 两个变更引发了指标数据不可用问题：一个与权限相关，另一个与调度系统相关。2024年1月3日11:23 PST，这些变更被推出，最初影响较小。但在1月9日14:07 PST尝试修复时，引发了更严重的问题，服务器重启率增加，导致数据不可用。		**硬件故障导致服务失效** （磁盘瓶颈） → （高延迟和失败）

14	2022-7-19 Incident began at **2022-07-19 06:33** and ended at **2022-07-20 21:20**	1 day, 15 hours	2022年7月19日06:33（美国太平洋时间），欧洲区europe-west2-a数据中心的多个冗余冷却系统同时发生故障，导致多个Google Cloud服务不可用。受影响的客户在故障期间无法正常使用相关产品。 区域影响 • 一些Google Cloud区域服务在此事件中受到影响，尽管这些服务是设计为能应对单个区域故障的。调查发现以下两个关键因素导致了区域服务的影响： 1. 事故初期，内部服务的流量路由配置被误改，导致流量避开了整个europe-west2区域的所有三个区域，而不仅仅是受影响的europe-west2-a区域。此问题于2022年7月19日12:35（美国太平洋时间）得到纠正。 2. Google的区域存储服务（如GCS和BigQuery）在多个区域中复制客户数据。由于路由变更，这些服务无法访问部分数据对象的副本，直到流量路由被修正后，客户才恢复对这些存储对象的访问。	europe-west2-a区域的一个数据中心由于多个冗余冷却系统的同时故障，以及极高的外部温度，无法维持安全的操作温度。为了防止更长时间的停机或设备损坏，Google决定关闭该数据中心的部分区域，这导致容量部分失效，实例终止、服务降级和网络问题随之发生，影响了部分客户。	冷却系统影响时长 Google工程师于2022年7月19日10:05（美国太平洋时间）关闭了部分受影响的europe-west2-a区域的数据中心，等待冷却系统的修复。冷却系统于14:13修复，总计影响时间为4小时8分钟。 云服务恢复时长 冷却系统修复后，Google工程师于2022年7月19日14:13（美国太平洋时间）开始恢复云服务。到7月20日04:28，云服务全部恢复正常，总计影响时间为18小时23分钟（从7月19日10:05到7月20日04:28）。 长尾影响时长 在初步恢复服务后，少数Google Compute Engine实例需要工程师进一步手动修复，导致这些实例以及依赖GCE的服务（如Cloud SQL）依然无法使用。这些服务在7月20日21:20（美国太平洋时间）全部恢复，总计影响时间为35小时15分钟（从7月19日10:05到7月20日21:20）。	**硬件故障导致服务失效** (冷却系统故障) → (设备关闭，服务失效)
15	2021-6-19 Incident began at **2021-06-19 23:00** and ended at **2021-06-23 09:06**	3 days, 10 hours, 6 minutes	2021年6月19日23:00至2021年6月23日09:06（美国太平洋时间），多个Google Cloud服务在us-east1-{a,b,c,d}、us-east4-{a,b}、us-west1-c和us-west4-a区域，遇到了与创建新Persistent Disk Solid-State Drive (PD-SSD) 设备相关的间歇性问题，持续时间为3天10小时6分钟。此次问题影响了依赖PD-SSD的服务，导致许多服务在创建新的资源时出现失败。	此次事件的根本原因是PD-SSD的利用率意外激增，导致部分区域的PD-SSD容量不足。这一容量限制影响了需要PD-SSD支持的服务和操作，导致这些服务在创建新资源时遇到间歇性失败或性能下降。	• **Google Compute Engine (GCE)**：用户在创建新虚拟机时遇到启动磁盘创建失败，自动扩容无法正常工作，部分用户遇到写入吞吐量下降的问题。 • **Google Kubernetes Engine (GKE)**：用户在创建新集群或扩展节点池时遇到间歇性问题。 • **Cloud Composer、Cloud SQL、Dataproc、Dataflow**：这些服务依赖PD-SSD，创建环境、集群或作业时遇到失败。 • **Cloud Build**：使用自定义大小VM或worker pools的构建作业出现失败。	**硬件故障导致服务降效、失效** （SSD容量不足）→（间歇性失败和性能下降）
16	2021-5-20 Incident began at **2021-05-20 05:25** and ended at **2021-05-20 16:10**	10 hours, 45 minutes	2021年5月20日05:25（美国太平洋时间），Google Cloud产品因访问控制列表（ACLs）问题，导致服务延迟和错误，持续时间为10小时45分钟。此次问题源于Google内部生产资源的权限定义出错，阻止了一些内部服务帐户访问生产作业，进而影响了下游服务。	Google的数据中心依赖于ACLs来执行各种操作，例如验证权限、激活新API或创建云资源。此次事件的根本原因是生产ACL系统中的一个潜在并发问题和缺少安全检查机制的结合，导致部分生产环境的ACL被截断。具体来说，ACL组件中的一个安全检查机制由于某些数据中心的版本更新而被错误禁用，导致无效ACL文件被处理。错误ACL文件导致部分组成员资格被意外删除，触发了广泛的服务故障。		**软件错误导致服务降效、失效** (访问控制列表设置错误) →（服务延迟和错误）
17	2020-3-26 Incident began at **2020-03-26 16:14** and ended at **2020-03-27 05:55**	13 hours, 41 minutes	2020年3月26日16:14（美国太平洋时间），Google Cloud的Identity and Access Management (IAM) 发生了高错误率问题，持续时间为3.5小时，导致多个服务中断。部分服务的管理操作数据在14小时内继续受到影响，原因是服务中使用了过时的数据。由于IAM在众多GCP服务中的核心作用，此次故障影响了许多下游服务。	IAM依赖分布式访问控制列表（ACL）来验证权限、激活新API或创建云资源。权限数据存储在分布式数据库中，并被大量缓存。两个进程负责保持数据库的最新状态：一个是实时进程，另一个是批处理进程。如果实时管道积压严重，缓存的过时数据可能会被用于处理请求，从而影响操作。 事件的起因是一次大规模的组成员更新，导致修改权限的数量远超预期，从而产生了大量的实时队列更新积压。缓存服务器因内存问题无法正常处理积压请求，导致IAM请求超时。在此期间，紧急更新进一步加重了部分区域的问题。	• **时间范围**：从2020年3月26日16:14至2020年3月27日06:20（美国太平洋时间），Cloud IAM使用了过时的数据，导致多种服务受到影响。 • **错误率高峰期**：16:35到17:45、18:45到19:00、19:20到19:40，部分区域错误率高达100%。 • **影响的服务**：多个Cloud服务在多个区域出现并发中断，且大多数区域均有受到不同程度的影响。 • **IAM成员权限**：使用Google Groups分配IAM角色的用户在此期间受到了权限过时问题的影响，而直接授予IAM角色的用户未受到影响。	**软件错误导致服务失效** (组员更新操作错误) → (服务中断)

18	021-07-21 Incident began at **2021-07-21 19:22** and ended at **2021-07-27 15:28**	5 days, 20 hours	2021年7月21日19:22（美国太平洋时间），Google Cloud Scheduler在向Pub/Sub主题发布消息时，全球范围内出现错误，持续时间为5天20小时6分钟。此次故障的根本原因是一项配置变更，更新了Cloud Scheduler发布到Pub/Sub时所使用的服务代理。由于某些项目未正确配置新的服务代理权限，导致出现“PERMISSION_DENIED”错误。	故障的根本原因是一项配置更改，该更改更新了Cloud Scheduler发布消息到Pub/Sub时所使用的服务代理。由于许多项目未向新的Cloud Scheduler Google管理的服务账户授予访问Pub/Sub主题的权限，导致这些项目中的调度任务在发布消息时触发了“PERMISSION_DENIED”错误。	• **影响范围**：所有区域的Google Cloud Scheduler任务在向Pub/Sub主题发布消息时出现了错误。 • **受影响的客户**：使用Pub/Sub作为Cloud Scheduler任务目标且未向新的服务账户授予访问权限的客户，均收到“PERMISSION_DENIED”错误，导致调度任务无法正常执行。	**软件错误导致服务失效**（配置错误）→(服务失效)
19	2023-11-27 Incident began at **2023-11-27 05:01** and ended at **2023-11-29 13:56**	2 days, 9 hours	2023年11月28日09:46（美国太平洋时间），Google Cloud SQL服务在MySQL 8.0.30+版本中启用了Query Insights时，出现了与多表DML操作相关的间歇性问题。问题主要影响到执行多表DML（例如“UPDATE tableA JOIN tableB”）的客户。问题在2023年11月29日13:55（美国太平洋时间）被完全解决。	问题发生在启用了Query Insights的Cloud SQL MySQL 8.0.30+版本中。多表DML（多表数据操作语言）是影响多个表的操作，例如JOIN操作。在此版本下，启用Query Insights时，这些多表DML操作间歇性失败，阻碍了正常的查询和数据修改操作。	• 受影响客户：所有使用Cloud SQL MySQL 8.0.30+并启用了Query Insights的用户，在执行多表DML操作时遇到了间歇性失败。 • 问题表现：多表DML操作（例如“UPDATE tableA JOIN tableB”）无法正常执行，影响了客户的数据操作。	**软件错误导致服务失效**(数据库版本错误)→(数据库服务失效)
20	024-7-30 Incident began at **2024-07-30 02:36** and ended at **2024-07-30 12:44**	10 hours, 8 minutes	2024年7月30日12:30（美国太平洋时间），Google Cloud VMware Engine的证书更新工作已完成，影响范围内的所有项目问题已解决。Google工程团队对NSX、V-Center和HCX虚拟机的证书进行了更新。此次事件的起因是DigiCert发现其域名控制验证（DCV）存在问题，要求所有相关证书必须在2024年7月30日19:30 UTC前撤销和更新。	DigiCert是Google Cloud VMware Engine Private Cloud中使用的证书颁发机构，负责签发数字证书。在此次事件中，DigiCert发现了其域名控制验证（DCV）中的问题，导致Google Cloud必须在最后期限前更新所有相关证书。更新过程涉及对NSX、V-Center和HCX虚拟机的证书进行更新。 证书更新的过程可能导致以下问题： 1. **现有备份和复制任务**可能会在更新期间失败。 2. **管理任务**（如节点添加/移除）在更新过程中无法执行。 3. 在证书更新后，**第三方产品**可能会因SSL指纹不匹配而出现问题。	• **受影响的服务**：NSX、V-Center、HCX虚拟机。 • **对客户的影响**：虽然对工作负载虚拟机的访问没有影响，但备份、复制和管理任务在证书更新期间可能会失败。第三方应用程序（如备份和复制工具）可能因SSL指纹不匹配而遇到问题。	**软件错误导致服务失效**(证书更新错误)→（服务失效)
21	2024-7-18 Incident began at **2024-07-18 23:48** and ended at **2024-07-19 16:32**	16 hours, 44 minutes	从2024年7月19日04:09 UTC开始，Google Cloud检测到部分客户的Windows虚拟机（VM）因CrowdStrike Falcon更新后出现了“蓝屏死机（BSOD）“ 和崩溃循环问题。这些问题是由CrowdStrike发布的一次错误更新引起的，导致运行CrowdStrike Falcon的Windows VM无法正常工作。CrowdStrike快速部署了修复程序，但部分客户仍然受到影响。	事件的起因是CrowdStrike Falcon发布的一次错误更新，导致部分Windows VM发生崩溃。具体来说，Windows VM在接收到有缺陷的CrowdStrike补丁后，会发生“蓝屏死机”（BSOD），并进入重启循环。这一问题影响了使用CrowdStrike Falcon的Windows VM。 错误补丁的根本原因是`Csagent.sys`（CrowdStrike应用程序包的一部分）的版本问题，导致系统发生“系统线程异常未处理”的错误（SYSTEM_THREAD_EXCEPTION_NOT_HANDLED），引发蓝屏崩溃。	• **影响范围**：运行CrowdStrike Falcon的Windows虚拟机。 • **主要表现**： 1. 受影响的Windows虚拟机崩溃，进入“蓝屏死机”（BSOD）状态，并可能无法重启。 2. **系统日志**中显示调用栈，主要涉及`Csagent.sys`驱动程序文件。 3. 80%的受影响VM可以在重启后自行恢复，部分需要手动修复。	**软件错误导致服务失效**（更新错误）→（机器宕机，服务失效)
22	2024-3-21 Incident began at **2024-03-21 09:29** and ended at **2024-03-25 08:32**	3 days, 23 hours	自2024年3月20日起，使用Google Distributed Cloud (GDC) Edge的客户在创建新的Google Kubernetes Engine (GKE)集群时遇到问题。受影响的客户在GDC Edge区域创建GKE集群时可能会遇到超时或内部错误，导致集群创建失败。现有集群未受到此次问题的影响。	此次问题的根本原因尚未完全公开，但工程团队已确定解决方案，并正在进行修复工作。问题主要影响的是尝试在GDC Edge区域创建新GKE集群的用户，出现超时或内部错误。	• **受影响的操作**：尝试在GDC Edge区域创建新的GKE集群时，客户可能遇到超时或内部错误，导致集群创建失败。 • **未受影响的操作**：现有的GKE集群未受到此次问题的影响，客户可以正常使用现有集群。	**未知错误导致服务失效**

23	2023-11-2 Incident began at **2023-11-02 10:45** and ended at **2023-11-10 13:37**	8 days, 4 hours	Google Kubernetes Engine (GKE) 的客户在启用**Workload Identity**功能后，可能会遇到应用日志记录速率过高的问题。虽然此问题不会影响集群的功能或性能，但会导致额外的日志被写入Cloud Logging，从而消耗日志配额，并可能产生超出免费配额的额外账单。	GKE的**gke-metadata-server**是GKE Workload Identity功能的一部分。版本**0.4.272到0.4.280**的gke-metadata-server存在配置错误，导致生成大量包含“Unable to sync sandbox”字符串的调试日志。这些日志被大量写入Cloud Logging，消耗了日志的摄取配额，可能会引发额外的账单。	• **受影响的操作**：启用**Workload Identity**的GKE集群会产生大量调试日志，消耗Cloud Logging的配额，可能会导致超出免费月度限额的额外账单。 • **未受影响的操作**：集群的功能和性能不会受到此问题影响，日志写入是唯一的影响。	**软件错误导致服务降效** (多版本的配置错误) → (消耗额外大量资源)
24	2023-10-2 Incident began at **2023-10-02 11:29** and ended at **2023-10-12 12:28**	10 days, 1 hour	Google Kubernetes Engine (GKE) 的少部分客户在手动升级Nodepool时遇到了失败问题。虽然所有其他Nodepool操作正常运行，且工作负载和Kubernetes API的使用未受影响，但极少数客户的Nodepool升级请求失败。目前，影响范围已减少到少于0.1%的Nodepool升级请求，主要集中在us-central-1、us-west-1、us-east-1、europe-west1、europe-west4和asia-northeast-1区域，之前的失败率曾达到0.4%。	此次问题的根本原因尚未完全公开，工程团队仍在积极修复。部分客户在尝试手动升级Nodepool时，可能会在Google Cloud控制台中看到“Internal error”提示，并且重试操作可能无法解决问题。	• **受影响的操作**：受影响客户在手动进行Nodepool升级时可能会遇到失败。此次问题仅限于极少数客户（<0.1%），且主要发生在us-central-1、us-west-1、us-east-1、europe-west1、europe-west4和asia-northeast-1区域。 • **未受影响的操作**：GKE工作负载、其他Nodepool操作及Kubernetes API使用未受到此次问题影响。	**未知错误导致服务失效**
25	2024-6-25 Incident began at **2024-06-25 11:58** and ended at **2024-06-28 12:22**	3 days	从2024年6月25日11:58（美国太平洋时间）到2024年6月28日12:22，Google SecOps服务在美国/多区域经历了服务降级，持续时间为3天23分钟。受影响的客户在使用SecOps的多个功能时遇到了问题。	此次事件的具体根本原因尚未公开，但涉及多个Google SecOps功能的故障，特别是用户界面、日志分析和数据摄取相关的问题。可能是系统配置或后台服务异常导致多个模块的功能同时受到影响。	在此次事件期间，受影响的客户可能遇到了以下问题： 1. **Parser UI**：用户无法通过用户界面访问解析器。 2. **Feeds UI**：Feed名称无法在用户界面显示，影响了相关功能的使用。 3. **Raw Log Search Timestamp Selector**：时间戳选择器限制了用户选择较早日期，影响了日志搜索功能。 4. **Raw Log Search UI**：原始日志搜索界面显示所有日志类型为0KB，导致无法进行准确的日志分析。 5. **Raw Log Search Historic Availability**：超过48小时后的历史数据搜索不可用。 6. **IOC Matches Page**：IOC匹配页面中，Feed源名称显示不正确。 7. **数据摄取**：部分第三方API源的数据摄取出现延迟。	**未知错误导致服务降效**
26	2024-9-25 Incident began at **2024-09-25 01:27** and ended at **2024-09-25 12:28**	11 hours, 1 minute	2024年9月25日01:27至12:28（美国太平洋时间），Mandiant Security Validation SaaS的客户无法创建或运行Actions、Sequences和Evaluations，持续时间为11小时01分钟。在01:27至11:22期间，客户可以登录并查看之前运行的结果，但无法创建或运行新内容。11:23至12:28期间，客户被重定向到维护页面，通知系统正在维护。	此次事件的根本原因是后端数据库中的一个实现问题，数据库中用于存储某些序列的列值超出了其限制。该列值的溢出导致数据库和系统出现错误，阻止了用户运行Actions、Sequences和Evaluations。	• **01:27至11:22 US/ Pacific**：客户能够登录并查看UI和之前运行的作业结果，但无法创建或运行新的Actions、Evaluations或Sequences。 • **11:23至12:28 US/ Pacific**：客户无法登录，被重定向到一个维护页面，通知系统正在修复问题。	**软件错误导致服务失效** （数据库设置超限）→（数据库服务失效）
27	2024-7-8 Incident began at **2024-07-08 23:20** and ended at **2024-07-12 06:31**	3 days, 7 hours	从2024年7月8日23:20（美国太平洋时间）到2024年7月12日06:31，**reCAPTCHA Enterprise**服务因客户端代码变更出现了问题，持续时间为3天7小时11分钟。该问题导致reCAPTCHA请求被错误地发送到客户服务器而非reCAPTCHA服务器，从而引发大量的4xx错误，部分客户因此无法正常使用reCAPTCHA服务。	问题的根本原因是**reCAPTCHA Enterprise**客户端代码中的一项变更，导致请求被发送到客户的服务器，而不是reCAPTCHA的服务器。这些请求指向了客户服务器上不存在的URI，导致了404错误。部分客户因为错误处理方式，使得reCAPTCHA功能对他们不可用。	• **错误请求**：受影响的客户会看到大量请求被发送到不存在的URI，导致出现404错误。 • **reCAPTCHA不可用**：部分客户由于错误的处理方式，使reCAPTCHA服务无法正常工作，影响了他们的应用功能。 • **影响范围**：全球范围内的reCAPTCHA Enterprise用户受到影响，大约50%的reCAPTCHA脚本受到影响，问题持续约10小时。	**软件错误导致连接中断** （代码缺陷）→（错误的URL请求）