阿里云、腾讯云 及其他云商 故障事件 截止2024.10

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

云中断造成损失越来越大，准备工作愈显重要

考虑到服务中断已经司空见惯，做好准备工作变得尤为重要。云服务巨头AWS在11月的re:Invent大会上宣布提供更多故障注入服务场景，方便客户测试应用程序在极端情况下的表现，比如某个云可用区完全断电或与另一可用区失去连接。

根据Parametrix Insurance今年发布的报告，AWS位于美国东部1区（us-east-1）的关键业务服务如果停机24小时，可能会导致34亿美元的直接收入损失，停机48小时可能会导致78亿美元的损失。该区域是服务《财富》世界500强公司数量最多的AWS区域。

根据报告，东部1区（east-1）和西部2区（west-2）AWS服务停机24小时可能会导致82亿美元的损失，停机48小时可能会导致175亿美元的损失。

Aviatrix预计将于明年1月发布的一份报告，将给担心威胁行为者会造成中断的IT专业人员提供更多数据。报告发现，“在过去一年中，由防火墙导致的云网络中断次数是组织内部遭遇的网络攻击次数的两倍多。”

参考资料：https://www.crn.com/news/cloud/the-15-biggest-cloud-outages-of-2023

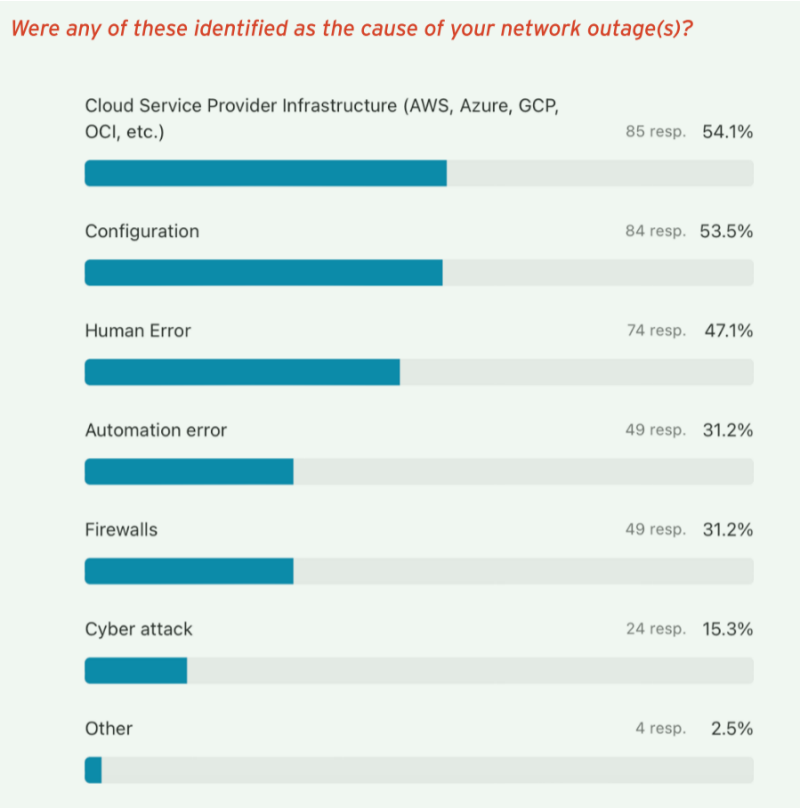
Aviatrix的2024发布的公开报告，今年的调查包括400多名全球受访者，涵盖安全、云和网络角色，其中一些人表示他们在组织中担任多个此类角色。超过一半的受访者来自员工超过2,000人的企业组织。

本报告将更仔细地研究这些调查结果的原因和影响，以及未来改善企业和行业成果的建议。

1）传统方法和落后的技能集是云安全问题的原因。在过去的一年中，防火墙（31.2%）比网络攻击（15.3%）造成的云网络中断更多。此外，人为错误导致了47.1%的中断。

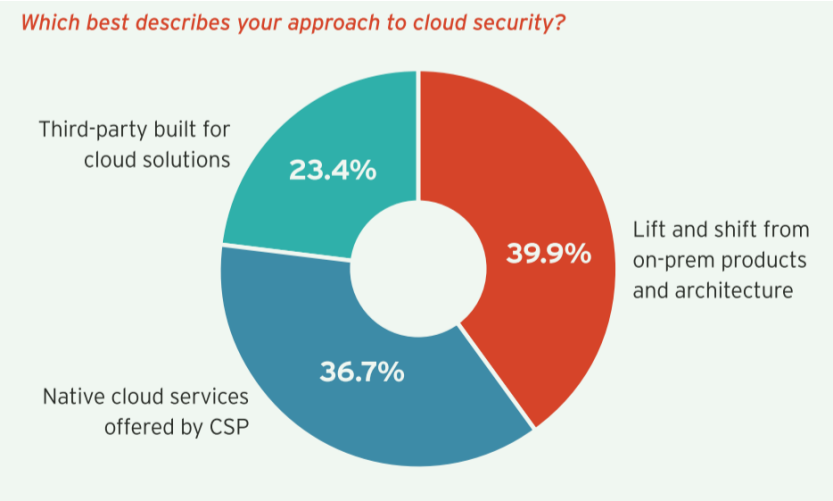
2）云网络中断是许多企业面临的另一个现实。超过三分之一（37.9%）的受访者表示，他们的公司在过去12个月内发生过云网络中断。

这些中断的原因是广泛的。超过一半的受访者将原因归咎于（54.1%）云服务提供商基础设施（AWS、Azure、GCP、OCI等），另有53.5%的人提到了配置问题，另有47.1%的人认为是人为错误，31.2%的人认为是自动化错误，31.2%的人认为是防火墙问题，15.3%的人认为是网络攻击问题。



3）根据这项调查，39.9%的受访者将他们的云安全方法描述为“提升和转变”。另有36.7%的受访者表示，他们依赖云服务提供商（CSP）提供的原生云服务。不到四分之一（23.4%）的受访者表示他们正在使用第三方云解决方案。

（According to this survey, 39.9% of respondents described their approach to cloud security as "lift and shift". Another 36.7% said they rely on native cloud services offered by cloud service providers (CSPs). Less than 1/4 (23.4%) report that they are using third-party built for cloud solutions.)



基于这些发现，大多数企业在迁移到云之后并没有重新定义他们的安全方法-相反，他们采取了内部部署的方法并将其应用于云部署。对于那些采用特定于云的安全方法的人来说，默认情况下是使用CSP本身提供的工具。

（Based on these findings, the majority of businesses have not redefined their approaches to security since moving to cloud – rather they've taken what worked on-prem and applied it to their cloud deployments. For those that have taken a cloud-specific approach to security, the default is to use the tools provided by the CSPs themselves.)

4）可见性和可预测性是云计算成本的关键挑战。根据这项调查，34.8%的组织在过去12个月内受到意外的云网络或安全成本的打击。在受影响的企业中，30.5%的企业表示意外成本为10万美元或以上，12.4%的企业表示意外云网络或安全成本超过50万美元。（图15）

（Visibility and predictability are key challenges when it comes to cloud costs. According to this survey, 34.8% of organizations have been hit with unexpected cloud networking or security costs in the past 12 months. (Figure 14) Of those impacted, 30.5% report those unexpected costs were $100,000 or more, with 12.4% citing upwards of $500,000 in unexpected cloud networking or security costs.)

Figure 14

Has your organization been hit with unexpected cloud networking or security costs in the past 12 months?

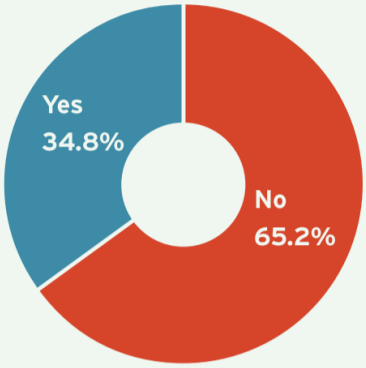
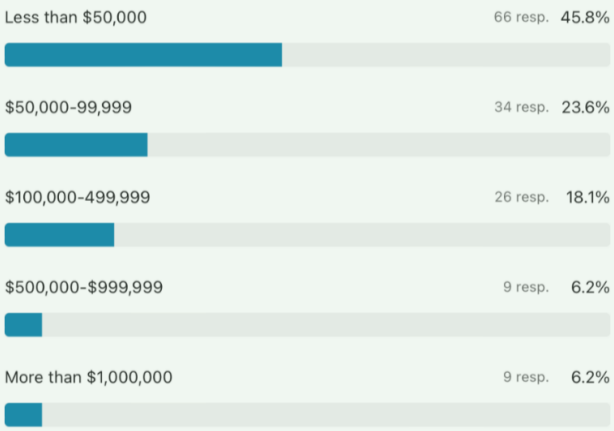


Figure 15

Approximately what amount of unexpected cloud networking or security cost did you incur within the past 12 months?



云计算成本的不可预测性和可变性无疑是云网络前线从业者的痛点。然而，从过去一年成本超支的数量和频率来看，这个问题远未解决。随着企业在未来几个月和几年内对云计算进行预算，深入了解其组织内的云计算使用和支出趋势至关重要，以制定切合实际的期望并实施云计算成本控制。

（The unpredictable and variable nature of cloud costs is undoubtedly a pain point for the practitioners on the front lines of cloud networking. However, it’ s clear from volume and frequency of cost overruns in the past year that this issue is far from solved. As businesses budget for cloud in the months and years ahead, it will be critical to get a deeper understanding of cloud usage and spending trends within their organizations to set realistic expectations and implement cloud cost controls.)

5）重新定义安全最佳实践，以充分利用云。正如从业者报告的那样，大多数企业在迁移到云计算后并没有重新定义其安全方法-大多数企业要么取消并转移了其内部部署方法，要么默认使用其CSP提供的工具。这些当前的方法导致了安全问题、云网络中断和错过云迁移最后期限。将安全方法现代化以构建云解决方案将通过设计改善云安全结果。接受调查的从业者还建议，组织应该关注云中网络和安全的融合，以简化操作并降低业务风险。

（Redefine security best practices to take full advantage of the cloud.

As practitioners report, the majority of businesses have not redefined their approaches to security since moving to cloud – the majority have either lifted-and-shifted their on-prem approach or are defaulting to tools provided by their CSPs.

These current approaches have led to security concerns, cloud network outages, and missed cloud migration deadlines. Modernizing security approaches to built-for-cloud solutions will improve cloud security outcomes by design.

Practitioners surveyed also suggest that organizations should look toward the convergence of networking and security in the cloud in order to simplify operations and reduce business risk.)

序号	事件名称	事件描述	故障分析	故障原因	缓解与恢复	故障在系统中的影响	故障归因
1	Facebook Outage	**北京时间 2021 年 10 月 4 日下午 4 点左右**，互联网巨头 facebook 及其附属应用程序 whatsapp 和 instagram 全面瘫痪。用户和企业开始注意到信息无法发送、图片无法发布以及他们的更新被置若罔闻，全世界都感受到了这一震撼性的数字事件。 这些路由器协调 facebook 数据中心之间的网络流量，基本上是 facebook 所有业务的基础。因此，故障对 "我们数据中心的通信方式产生了连锁反应，导致我们的服务停止"。 从技术上讲，真正的故障是边界网关协议（bgp）的撤销。**(CFG error and router breakdown and service disconnected)** 从本质上讲，边界网关协议是驱动互联网的巨大服务器的集合，它们不断更新并在网络上共享信息，并接入我们所看到的互联网--一个由网络组成的网络。 注：一般来说，在对服务进行更改时，确定风险因素至关重要。					**软件错误导致连接中断** （网关协议配置错误）→(连接中断)
2	阿里云香港机房制冷故障	**2022年12月18日**，阿里云香港机房制冷设备故障，导致多个香港及澳门的站点受到影响，宕机时间超过10个小时。**(hardware failure and hosts breakdown and service breakdown)** “由于阿里云的香港机房节点发生故障，导致澳门金融管理局、澳门银河、莲花卫视、澳门水泥厂等关键基础设施营运者的网站、澳觅和MFood等外卖平台以及澳门日报等本地传媒应用程式，自今天（18日）中午开始暂时无法访问使用。 ”	2022年12月19日下午，根据最新的更新进展显示，目前阿里云所租用的香港电讯盈科公司机房已修复制冷设备故障，阿里云香港地域所有可用区云产品功能正在陆续恢复正常。 此次故障，影响香港地域可用区c的云服务器ecs、云数据库、存储产品（对象存储、表格存储等）、云网络产品（全球加速、nat网关、vpn网关等）等云产品使用。 这一故障也影响了香港地域控制台访问和api调用操作。 对于受本次故障影响的产品，阿里云将根据相关产品的sla协议进行赔付。 可见，这次已超过24小时的服务器宕机，为各网站及平台造成巨大损失，让阿里云惨遭滑铁卢。 多位阿里云用户宕机时间超过24小时，部分用户直到19日中午才得以恢复。另有电商用户表示，其宕机超过28小时仍未恢复。 “从昨天早上11点开始，打了11次售后电话。但却一直无人回电。”		2022年12月25日，阿里云发布《关于阿里云香港Region可用区C服务中断事件的说明》，复盘了该事件的处理过程、服务影响、问题分析以及改进措施等。涉及到的问题包括：冷机系统故障恢复时间过长、现场处置不及时导致触发消防喷淋、客户在香港地域新购ECS等管控操作失败、故障信息发布不够及时透明。		**硬件故障导致服务失效** （机房制冷故障）→(机房设备关闭，服务失效)
3	腾讯云广州机房制冷故障	**2023年3月底**，微信、QQ等业务也曾出现大面积功能异常，涉及到微信的异常包括语音呼叫、账号登录、朋友圈以及支付在内的多个功能无法正常使用，QQ文件传输、QQ空间、QQ邮箱等也同样出现问题。 腾讯客服官方微博于3月29日凌晨3点30分发布消息称，由于系统故障，部分用户使用微信支付相关功能出现异常，当天上午10点50分，腾讯微信团队宣布，微信、微信支付相关功能已恢复。	据媒体报道，此次事故由广州电信机房冷却系统故障导致，腾讯将其定义为公司一级事故，多个管理层因此受到通报批评和处罚。**(hardware failure and service breakdown)**		4月12日，工业和信息化部信息通信管理局听取腾讯公司关于“3·29”微信业务异常情况汇报，要求腾讯公司进一步健全安全生产管理制度、落实网络运行保障措施，坚决避免发生重大安全生产事故，切实提升公众业务安全稳定运行水平。		**硬件故障导致服务失效**
4	腾讯云云监控控制台部分功能异常	**问题陈述 2023 年 4 月 18 日星期三**，云监控平台中生产环境使用的数据库实例 IP 出现问题。 因此，云监控控制台的某些部分出现功能异常。 该问题从 17:00 持续到 17:43 UTC+8。 云监控服务的异常状态给您带来了不便，对您的用户体验造成了负面影响，我们对此深表歉意。 **事件背景** 在云监控平台的生产环境中，发生了一起不幸事件，即在迁移过程完成之前，数据库实例被错误地从其迁移标识符中分离出来。 **(human operation error and network failured and database service disconnected)** 结果，没有必要标识符的数据库无法通过旧 IP 地址访问，尤其是在高负载高可用性（HA）切换场景中。 这导致生产环境服务中的数据库连接异常。	**切换不成功的具体原因是什么？** 高负载情况促使对 CDB 进行例行高可用性主从切换。 但是，数据库实例尚未完成迁移，被错误地标记为已迁移。 结果，先前的虚拟 IP (VIP) 在切换过程中失效，只能访问新的 VIP。 这一差异导致旧 IP 的数据库连接异常。 因此，任何尚未完全过渡到新 IP 的流量都无法访问数据库，导致连接失败和随后的服务不可用。		**事件发生期间发生了什么？** 1. 事件开始时间： UTC时间16:38，群集触发高负载警报，显示 CPU 使用率超过95%。 2. 事件触发： 16:38 UTC 时，缓慢查询的发生率开始上升。 16:58 UTC 时，业务层的成功率随之下降。与此同时，缓慢查询的数量达到峰值。 3. 故障排除过程： 故障排除过程包括检查业务层的服务日志。 发现一个特定的数据库 IP 出现异常访问。 经调查，确定与该 IP 相关的数据库实例一直处于高负载状态，并进行了高可用性故障切换，导致旧 IP 失效。随后的调查显示，该实例被错误地标记为已迁移。 4. 采取的措施： - 扫描配置中心中使用旧 IP 的所有配置，并将数据库访问 IP 地址更新为可用 IP 地址： 恢复数据库访问后，业务层服务界面的成功率提高，云监控控制台的功能恢复正常。	**影响** 1. 警报控制台无法运行，影响警报历史显示，妨碍用户执行常规控制台操作。 2. 警报通知在检索警报通知信息内容时遇到问题，导致无法按预期发送警报通知。 3. 控制面板控制台无法访问，导致用户无法访问监控数据，并显示显示操作失败的错误信息。	**软件错误导致连接中断** （人为维护操作失误）→(数据库服务连接中断)
5	阿里云双十一 全线故障	**2023年11月12日**，阿里云故障导致阿里系App（小写）全线“崩”上热搜，涉及到阿里云盘、淘宝、咸鱼、钉钉、语雀等等产品。 阿里云官网通告显示，故障开始于11月12日傍晚，持续时长约3个半小时。	17:44分，阿里云监控发现云产品控制台访问及API调用出现异常，阿里云工程师正在紧急介入调排查。 17:50分，阿里云已确认故障原因与某个底层服务组件有关，工程师正在紧急处理。**(software Bug and service breakdown)** 18:54分，杭州、北京等地域控制台已经恢复，其他地域控制台服务逐步恢复中。 19:20分，工程师通过分批重启组件服务，绝大部分地域控制台及API服务已恢复。 “19:20左右，经工程师紧急处理，阿里旗下淘宝、钉钉、阿里云盘等App（小写）已全面恢复。”。 19:43分，异常管控服务组件均已完成重启，除个别云产品（如消息队列MQ、消息服务MNS）仍需处理，其余云产品控制台及API服务已恢复。 20:12分，北京、杭州等地域消息队列MQ已完成重启，其余地域逐步恢复中。 21:11分，受影响云产品均已恢复，因故障影响部分云产品的数据（如监控、账单等）可能存在延迟推送情况，不影响业务运行。 11月13日上午，查询阿里云官网显示，阿里云11月12日故障受影响地域包括：华北2 (北京)、华北6 (乌兰察布)、 华北1 (青岛)、华东2(上海)、华南2(河源)、华北3(张家口)、中国香港、印度(孟买)、美国(硅谷)、华南1(深圳)、英国(伦敦)、韩国(首尔)、日本(东京)、阿联酉(迪拜)、西南1 (成都)、华南3 (广州)、新加坡、澳大利亚 (悉尼)、马来西亚(吉隆坡)、 华北5 (呼和浩特)、 印度尼西亚(雅加达)、美国 (弗吉尼亚)、菲律宾 (马尼拉)、泰国(曼谷)、华东1(杭州)、华南1金融云。			此次故障影响了计算、容器、存储、网络与CDN、安全、中间件、数据库、大数据计算、人工智能与机器学习、媒体服务、企业服务与云通信、物联网、开发工具、迁移与运维管理等产品线内的上百个产品及服务。	**软件错误导致服务失效** （底层组件故障）→（多个服务失效）

6	腾讯云API系统故障	**2024年4月8日**，下午 15:31 分起，腾讯云管控面挂了，症状几乎和 **去年双十一阿里云史诗级大故障** 一毛一样：CVM 虚拟机，RDS 数据库还可以正常运行，但是管控面，特别是和对象存储 COS 与 Auth 有关的无一幸免。	官方报告显示，此次腾讯云服务故障的核心症结在于云API系统的异常。云API作为云上统一的开放接口集合，是客户通过编程方式管理和操控云端资源的关键通道，同时也是云控制台实现交互式网页功能的基石。当云API出现异常，直接影响了客户对云资源的正常访问与操作，导致云控制台登录困难，进而引发了一系列连锁反应。 依赖云API提供产品能力的多项公有云服务受到了直接影响，功能无法正常使用。受影响的服务清单涵盖了云函数、文字识别、微服务平台、音频内容安全、验证码等多个核心业务板块。这些服务的中断，无疑给依赖腾讯云服务的企业和个人用户带来了不同程度的运营困扰，尤其是对于那些高度依赖云函数进行业务逻辑处理、依赖文字识别和音频内容安全功能进行内容审核、以及依赖微服务平台进行业务集成和扩展的用户来说，影响尤为显著。 故障持续近87分钟，期间共有1957个客户上报了问题，反映了此次故障的广泛影响范围和严重程度。然而，腾讯云在情况说明中强调，尽管“酒店前台”（即控制台）出现故障，导致部分管理能力暂时瘫痪，但“已入住的客房”（即已配置好的服务器等IaaS资源，以及已经部署运行的业务）并未受到直接影响。这意味着，尽管客户在故障期间可能无法通过控制台进行资源管理、新增或调整操作，但已经部署在云上的业务系统和服务在很大程度上保持了稳定运行，未因此次云API异常而中断。			**软件错误导致连接中断** （云API系统异常）→(控制台服务连接中断)
7	阿里云机房火灾	2024年09月13日 11:32 北京，阿里云位于新加坡的数据中心遭遇严重故障，导致部分用户服务中断，包括网站访问缓慢、API调用失败、云存储服务不可达等一系列问题。而这一故障的背后，竟然是我们多有耳闻的——**机房火灾**。	据悉，此次故障发生于9月10日上午10:20分，是因新加坡机房发生火灾导致的升温。**(hardware failured and hosts breakdown and service breakdown)** 当时，阿里云监控发现新加坡地域可用区C网络访问出现异常，部分云产品服务出现异常。随后，阿里云工程师采取了紧急处理措施，而消防人员也第一时间赶往现场进行处置。经过30多个小时的紧张扑救，火势才得以控制。 阿里云表示，今日凌晨，大部分受到网络影响的云产品已恢复正常服务，但剩余断电的机房业务仍需等待物理条件的恢复。直到昨晚20:23分，消防部门仍在处理大楼现场风险中，运维工程师正在等待获准进入机房大楼。 同时，阿里云指出，如现场评估后不具备原地恢复的物理条件，应急小组将执行服务器设备迁移恢复预案。			• 进展更新】9月16日14:00，机器设备的安全迁移工作仍在稳定推进中，剩余受影响的云产品服务正在陆续恢复。由于部分机器仍处于危楼封锁区域无法进入，一些机器设备需要仔细干燥以确保数据安全，因此长尾机器的恢复可能持续较长时间。您可随时联系我们的工作人员，了解具体恢复情况。 • 【进展更新】09月14日19:00，已迁移完成的部分机器设备正在进行必要的上架准备工作，包括机器干燥、布线、上电、验证、调试等。 • 【进展更新】09月13日18:30，一层硬件设备正在安全迁移进行中。运维人员已获准进入二楼，完成勘查工作，在保全工作后将启动二层机器设备的安全迁移。 • 【进展更新】09月12日17:25，运维人员已获准进入大楼一层区域，正在现场评估安全迁移条件，并对硬件设备进行紧急保全。 • 【进展更新】09月11日20:23，消防部门仍在处理大楼现场风险中，运维工程师正在等待获准进入机房大楼。如现场评估后不具备原地恢复的物理条件，应急小组将执行服务器设备迁移恢复预案。 • 【进展更新】09月11日凌晨，大部分受到网络影响的云产品已恢复正常服务。剩余断电的机房业务仍需等待物理条件的恢复。 • 【进展更新】09月11日01:46，接当地消防要求，因消防浇水持续进行，机房开始出现积水和渗漏，电路存在短路风险，新加坡可用区C 一栋机房大楼整体紧急断电，可用区C其他大楼业务网络已陆续恢复。 • 【进展更新】截至09月10日20:04，目前火警仍未完全解除，受消防安全控制影响，运维工程师无法进入当地机房大楼，包间温度持续升高风险暂无法解除。目前机房部分网络设备在高温环境下已出现异常，影响部分云产品的网络互通。若后续温升未得到有效控制，新加坡可用区C整体脱网的可能性在增加。若您的业务部署在新加坡可用区C，我们将协助您尽快进行业务迁移。 • 【进展更新】09月10日14:40，受影响机房包间的火情已经基本得到控制，机房温度仍高。部分OSS对象存储、数据库等产品的单AZ版本，需待受影响物理机柜具备重新开机条件后恢复。其余高可用版本的云产品均已完成主动迁移。 • 【进展更新】截至09月10日12:15，按照产品调度策略，云原生大数据计算服务MaxCompute 已完成容灾切换。 • 【进展更新】截至09月10日11:30，按照产品调度策略，云数据库Redis/MongoDB/RDS MySQL、对象存储OSS、表格存储OTS等云产品的高可用版本已陆续完成容灾切换。 • 【进展更新】 异常因新加坡机房锂电池爆炸导致火灾及升温，消防人员已到达现场处置中，云网络大部分产品及云安全产品于09月10日10:55已完成主动切换，其他云产品服务仍在处理中。请您尽快迁移业务。	**硬件故障导致服务失效** （火灾导致机房设备关闭）→ (多个服务失效)
8	华为云网络故障	2022年6月13日，一条“同花顺崩了”的消息登上微博热搜。部分客户反映同花顺出现了无法进入页面交易、界面卡顿等情况。据悉，此次故障是由于为其提供相关服务的华为云产生了故障导致，从而引发了市场对于云计算服务的担忧。 基于此，华为云官方微博当日发布通知表示：2022年6月13日10:45-11：19，华为云检测发现华为云华南-广州区域公网访问异常，目前故障已排除、服务已恢复，问题根因正在进一步定位中。同时了解到华为云内部已经成立专项组分析故障原因。					**网络故障导致服务失效**
9	华为云北京区服务器宕机	2020年华为云发布公告称，4月10日上午检测到部分主机异常，目前故障基本修复，部分客户的业务正在配合恢复中。		华为云北京的机房出现了一些故障		4月10日，华为云疑似出现宕机，部分公司业务无法正常维持，有网友发帖称：“公司在华为云上的集群和服务全部挂了。” 据微博多位网友反映，从早上9点20分开始，华为云出现故障，华为云登录、管理后台无法访问。 晒图来看，不少使用云服务的后台都出现了“服务器暂时过载或处于维护中，请稍后重试。”“建立数据库连接时出错”等提示。	**硬件故障导致服务失效** （地区机房故障）→（服务失效）

10	2月甲骨文、NetSuite服务中断	2023年，甲骨文联合创始人兼首席技术官Larry Ellison曾公开表示，旗下甲骨文云基础设施（OCI）“不会崩溃”。但据Network World报道，2月OCI发生了一次持续数日的服务中断。 问题始于美国太平洋标准时间2月13日周一上午大约10:30，并持续到2月15日周三下午大约3:30，主要影响美洲、澳大利亚、亚太、中东、欧洲和亚洲的用户。		事件原因是，支持OCI公共域名系统API接口的后端基础设施出现性能问题，导致无法处理一些传入服务请求。甲骨文使用了实时后端优化和DNS负载管理微调来减轻问题。		根据Network World的报道，中断期间，OCI Vault、API Gateway、Oracle Digital Assistant和使用OpenSearch的OCI Search都出现了问题。 Data Centre Dynamics报道称，**甲骨文子公司NetSuite在美国东部标准时间2月14日中午左右发生服务中断，原因是马萨诸塞州沃尔瑟姆的Cyxtera数据中心起火。** 据The Register报道，Cyxtera数据中心切断了服务器电源，账户恢复工作大约在美国东部标准时间晚上10:26左右开始。 至少有一位Reddit用户报告称他们的账户因服务中断获得了一些抵扣券。 根据CRN 2023年统计数据，NetSuite在全球约有880个渠道合作伙伴，其中有300个位于北美。	**硬件故障导致服务失效** （数据中心起火）→ (服务器关闭，服务失效)
11	**4月甲骨文中心问题**	2023年，据Federal News Network报道，4月17日，美国退伍军人事务部遭遇甲骨文中心电子健康记录（EHR）系统中断，中断持续五个小时，起因是数据库能力升级和故障转移。 随后，在4月25日，甲骨文中心系统再次遭遇了近四个小时的中断，影响到了美国退伍军人事务部、美国国防部和美国海岸警卫队。 据报道，美国退伍军人事务部决定暂停进一步使用该系统，直到使用该系统的五个部门站点对系统功能性恢复信心为止。						**软件错误导致服务失效** （数据库升级错误）→ (多个服务失效)
12	**Salesforce中断问题**	2023年，Salesforce发布一份报告称，该供应商于9月20日遭遇服务中断，持续大约两小时，影响了其产品和服务。但MuleSoft和Tableau受到的影响时间长达约四小时。 根据公司的审查报告，这次中断是由于一项政策变更而意外引发的，该变更是“我们持续审查和更新安全控制的标准操作流程的一部分”。 报告称：“虽然这项变更旨在增强防御深度，但无意中阻止了对其意图范围之外的其他合法和必要资源的访问。最终结果是，访问权限不足导致服务之间通信中断，进而在我们系统内部产生了故障。这导致部分客户无法登录和使用服务。” 作为供应商，Salesforce已经修改了其变更审查和批准流程，并修复了Tableau中的启动竞争条件错误，以防止类似问题再次发生。Salesforce还承诺： “启用专门的自动化部署流程，以强制执行分阶段政策部署”，“启用额外的监控和警报功能，以更快地诊断与策略相关的问题”，并“对MuleSoft CloudHub的后端组件进行重新架构……以增强弹性。”						**软件错误导致连接中断** （政策变更错误）→ (服务间通信中断)