

腾讯云可观测平台 故障处理 产品文档







【版权声明】

©2013-2023 腾讯云版权所有

本文档(含所有文字、数据、图片等内容)完整的著作权归腾讯云计算(北京)有限责任公司单独所有,未经腾讯云事先明确书面许可,任何主 体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯,腾讯云将依法采取措施追究法 律责任。

【商标声明】

🔗 腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标,依法由权利人所有。 未经腾讯云及有关权利人书面许可,任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为,否则将构成对腾讯云及有 关权利人商标权的侵犯,腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况,部分产品、服务的内容可能不时有所调整。 您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则,腾讯云对本文档内容不做任 何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务,及相应的技术售后服务,任何问题请联系 4009100100。



文档目录

故障处理

云服务器 CPU 或内存占用过高 云服务器实例无法登录 云服务器带宽使用率过高 云服务器无监控数据 未收到告警



故障处理 云服务器 CPU 或内存占用过高

最近更新时间: 2022-04-28 20:28:42

简介

本文档介绍因云服务器 CPU 或内存占用过高,导致无法登录 Windows 和 Linux 云服务器实例的排查方法和解决方案。

排查思路

1. 登录实例定位消耗 CPU 或内存的具体进程。

- 2. 对 CPU 或内存占用率高的进程进行分析。
- 如果是异常进程,可能是病毒或木马导致,您可以自行终止进程,或者使用安全软件进行查杀。
- 如果是业务进程,则需要分析是否由于访问量变化引起,是否存在优化空间。
- 如果是腾讯云组件进程,请 提交工单 联系我们进一步定位处理。

故障定位及处理

针对 Windows 服务器

使用 VNC 方式登录云服务器

() 说明

由于云服务器负载高时会导致无法建立远程连接,推荐使用 VNC 方式登录 Windows 实例。

1. 登录 云服务器控制台。

2. 在实例的管理页面,找到目标云服务器实例,单击**登录**。如下图所示:

实例							实例使用指南 🖸
广州(6) • 上海(0) :	北京(0) 成	都(1) * 重 庆(1)	中国香港(0) 新加坡(0)	曼谷(0) 孟买(0)	首尔(0) 东京(0)	硅谷(0) 弗吉尼亚(0) 多	5伦多(0) 法兰克福(0) 莫斯科(0)
新建 开机 关机 所属项目:全部项目 关键字用"	N, 重启 "分隔,过滹标签	续费	聖置密码 更多操作 ▼			Q. 日童看待回收实例	\$ \$ ±
ID/实例名	监控	状态 ▼	主机类型 ▼	主IP地址	实例计费模式 ▼	网络计费模式	操作
	,lı	∪运行中	标准型82	(公) 「1 (内)	包年包月 2019-08-25 15:24到期	按带宽包年包月计	十费 登录 读费 更多 ▼
- 100 Jan	di	(1) 运行中	标准型S2	(建性)	包年包月 2019-09-26 14:23到期	按带费包年包月计	十费 登录 续费 更多 ▼

- 3. 在弹出的 "登录Windows实例" 窗口中,选择其它方式(VNC),单击立即登录,登录云服务器。
- 4. 在弹出的登录窗口中,选择左上角的 "发送远程命令",单击 Ctrl-Alt-Delete 进入系统登录界面。如下图所示:



发送远程命令	连接成功。如需粘贴命令,请点击 <u>这里</u>
Ctrl-Alt-Delete	
Ctrl-Alt-Backspace	
Ctrl-Alt-F1	按 Ctrl + Alt + Delete 登录。
Ctrl-Alt-F2	

查看进程占用情况

1. 在云服务器中,右键单击 任务栏,选择任务管理器。如下图所示:

			工具栏(の)	•
			层叠窗口(D) 堆叠显示窗口(E) 并排显示窗口(I) 显示编页(S)	
			任务管理器(K)	
	-		锁定任务栏(L) 属性(R)	
2	1			

2. 在打开的 "任务管理器" 中,即可查看资源占用情况。如下图所示:



₽ EASE 100 CES 200	理器		_ D X
文件(F) 选项(O) 查看(V)			
进程 性能 用户 详细信息 服务			
	* 1%	25%]
名称	CPU	内存	
■ 系统中断	0.5%	0 MB	^
Client Server Runtime Process	0%	0.8 MB	
▷ 1월 任务管理器	0%	6.0 MB	=
🔟 System	0%	0.1 MB	
📰 桌面窗口管理器	0%	15.1 MB	
▷ 🔳 BaradAgent (32 位)	0%	2.6 MB	
📧 Client Server Runtime Process	0%	1.0 MB	
▷ 🔟 Local Security Authority Proc	0%	2.9 MB	
🔟 Microsoft IME	0%	0.9 MB	
▷ 🏠 Microsoft 分布式事务处理协调	0%	1.6 MB	
▷ 🔳 sgagent (32 位)	0%	1.4 MB	
📧 TCP/IP Ping 命令 (32 位)	0%	0.6 MB	~
			结束任务(E)

🕛 说明

您可单击 CPU 或内存,以升序/降序对进程进行排序。

进程分析

根据任务管理器中的进程,分析与排查问题,以采取对应解决方案。

占用大量 CPU 或内存资源的进程为系统进程

如果您发现系统进程占用了大量 CPU 或内存资源,请排查以下内容:

1. 检查进程名称。

部分病毒会使用与系统进程相似的名称,例如 svch0st.exe、explore.exe、iexplorer.exe 等。

2. 检查进程对应的可执行文件的所在位置。

系统进程一般位于 C:\Windows\System32 目录下,并且会有完善的签名和介绍。您可以在任务管理器中,右键单击待查看的进程,选择



打开文件位置,即可查看具体可执行文件的位置。例如 svchost.exe 。如下图所示:

P		任	务管理	器			_ D >	¢
文件(F) 选项(O) 查看	¥	信束任务(E)						
进程 性能 用户 详细	ś	吉束进程树(T)						
	ì	殳置优先级(P)	•	2	c₽u	内存(专用	描述	~
VDLive.exe	1	设置相关性(F)		EM	00	956 K	YunJing Re	Π
QQPCSoftCmd.exe	5	分析等待链(A)		inistr	00	352 K	- 电脑管家-软	
svchost.exe	l	JAC 虚拟化(V)		AL SE	00	1,956 K	Windows 服	
👂 QQLive.exe	ť	创建转储文件(C)		inistr	00	812 K	腾讯视频	
💷 svchost.exe	ł	打开文件位置(O)		AL SE	00	2,784 K	Windows 服	
💷 svchost.exe	I	朕机搜索(N)		EM	00	508 K	Windows 服	
svchost.exe	J	 重性(R)		WOR	00	588 K	Windows 服	
🔁 powershell.exe	4	转到服务(S)		inistr	00	972 K	Windows P	
svchost.exe	3208	正住运行	545	EM	00	460 K	Windows 服	
QQPCTxtExt.exe	1996	正在运行	Adm	ninistr	00	180 K	电脑管家-Tx	
🖉 msdtc.exe	1448	正在运行	NET	WOR	00	16 K	Microsoft	
ChsIME.exe	2348	正在运行	Adm	ninistr	00	56 K	Microsoft I	
smss.exe	216	正在运行	SYS	TEM	00	40 K	Windows 会	
🖶 spoolsv.exe	368	正在运行	SYS	TEM	00	772 K	后台处理程…	=
svchost.exe	552	2 正在运行		TEM	00	688 K	Windows 服	
📧 wininit.exe	372	正在运行	SYS	TEM	00	308 K	Windows 启	
💷 winlogon.exe	400	正在运行	SYS	TEM	00	52 K	Windows 登	\sim
							结束任务(E)

- 如果进程位置不在 C:\Windows\System32 目录下,则表示该云服务器可能中了病毒,请手动或者使用安全工具进行查杀。
- 如果进程位置在 C:\Windows\System32 目录下,请重启系统或关闭不需要且安全的系统进程。

常见的系统进程如下:

- System Idle Process:系统空间进程,显示 CPU 空闲时间百分比
- system:内存管理进程
- explorer:桌面和文件管理
- iexplore: 微软的浏览器
- csrss: 微软客户端/服务端运行时子系统
- svchost:系统进程,用于执行 DLL
- Taskmgr: 任务管理器
- Isass:本地安全权限服务

占用大量 CPU 或内存资源的进程为异常进程

如果您发现一些命名很奇怪的进程占用了大量 CPU 或内存资源,则可能为木马病毒进程,例如 xmr64.exe(挖矿病毒)等。建议您使用搜索 引擎进行搜索,确认是否为木马病毒进程。

- 如果是木马病毒进程,请使用安全工具进行查杀,必要时考虑备份数据,重装系统。
- 如果不是木马病毒进程,请重启系统或关闭不需要且安全的进程。

占用大量 CPU 或内存资源的进程为业务进程

如果您发现业务进程占用了大量 CPU 或内存资源,例如 IIS、HTTPD、PHP、Java 等,建议进一步分析。

例如,判断当前业务量是否较大。

- 若业务量较大,建议您 升级服务器配置;若不升级服务器配置,可以考虑业务程序是否存在优化空间,请进行优化。
- 若业务量不大,则需要进一步结合业务报错日志来分析。例如,参数配置不当导致空耗资源。

占用大量 CPU 或内存资源的进程为腾讯云组件进程

请 提交工单 联系我们进行进一步定位处理。



Б

针对 Linux 服务器

登录云服务器

根据实际需求,选择不同的登录方式登录云服务器。

• 通过第三方软件远程登录 Linux 云服务器。

△ 注意

Linux 云服务器处于 CPU 高负荷状态时,可能出现无法登录状态。

• 使用 VNC 登录 Linux 实例。

△ 注意

Linux 云服务器处于 CPU 高负荷状态时,控制台可以正常登录。

查看进程占用情况

执行以下命令,查看系统负载,并根据 %CPU 列与 %MEM 列,确定占用较多资源的进程。

top

分析进程

根据任务管理器中的进程,分析与排查问题,以采取对应解决方案。

- 如果是业务进程占用了大量 CPU 或内存资源,建议分析业务程序是否有优化空间,进行优化或者 升级服务器配置。
- 如果是异常进程占用了大量 CPU 或内存资源,则实例可能中毒,您可以自行终止进程或者使用安全软件进行查杀,必要时考虑备份数据,重 装系统。
- 如果是腾讯云组件进程占用了大量 CPU 或内存资源,请 提交工单 联系我们进行进一步定位处理。
 常见的腾讯云组件有:
- sap00x: 安全组件进程
- Barad_agent: 监控组件进程
- secu-tcs-agent:安全组件进程

终止进程

- 1. 根据分析的占用资源的进程情况,记录需要终止的进程 PID。
- 2. 输入 k 。
- 3. 输入需要终止进程的 PID ,按 Enter。如下图所示: 此处以终止 PID 为23的进程为例。



									at 0.0F	_
Tacke	351 tota	up 5. 1	1 min	, 1 use	F, 10a0	a averaş ning	ge: 0.0	0, 0.0 ved.	9 zowbie	
2Coufel): 88	e. 1	a 1 👳		ni. 99 9	pring, Pring,	8 8 LB.	реа, аа	hi. A A ei. A A et	
KiB Mea	1879	516	total	14412	92 free	1270	368 use	4. 3	392156 buff/cache	
KiB Sue	m: 2097	148	total	20971	48 free	, 2010	9 II SP	a 15	537932 auail Mem	
PID to	simal/k	111	[defa	ult nid	= 2931	23	0 030	a. 15	SSISSE avair field	
PID	USER	PR	NI	UIRT	RES	SHR S	S ZCPU	ZMEH	TIME+ COMMAND	
293	root	20	8	8	8	0.5	\$ 0.2	0.0	0:03.24 kworker/2:1	
524	root	20	ø	Ø	0	0 5	S 0.1	0.0	0:03.53 kworker/0:2	
137	root	20	0	Ø	Ø	0 5	S 0.1	0.0	0:02.70 rcu sched	
141	root	20	0	0	0	0 5	S 0.0	0.0	0:00.73 rcuos/3	
15672	root	20	8	130156	2028	1260 J	R 0.0	0.1	0:04.61 top	
1	root	20	0	57592	7436	2612 3	S 0.0	0.4	0:03.44 systemd	
310	root	20	0	0	0	0 3	s 0.0	0.0	0:00.64 kworker/u256:1	
333	root	20	0	0	0	0 3	S 0.0	0.0	0:00.26 kworker/3:1	
540	root	20	0	0	0	0 5	S 0.0	0.0	0:00.11 jbd2/sda2-8	
619	root	20	0	43016	2876	2564 3	S 0.0	0.2	0:00.33 systemd-journal	
738	root	20	0	329592	23192	6252 3	S 0.0	1.2	0:01.02 firewalld	
745	root	20	0	19284	1236	944 \$	S 0.0	0.1	0:00.67 irgbalance	
754	dbus	20	0	34880	1904	1420 \$	S 0.0	0.1	0:00.27 dbus-daemon	
853	root	20	0	509040	9620	5956 3	S 0.0	0.5	0:00.30 NetworkManager	
901	polkitd	20	0	514364	12260	4568 3	S 0.0	0.7	0:00.17 polkitd	
1816	root	20	0	91064	2064	1064 3	S 0.0	0.1	0:00.09 master	
15681	root	20	0	0	0	0 3	S 0.0	0.0	0:00.06 kworker/1:1	
15699	root	20	0	0	0	0 5	S 0.0	0.0	0:00.01 kworker/1:0	
2	root	20	0	0	0	0 3	S 0.0	0.0	0:00.09 kthreadd	

△ 注意

若按 Enter 后出现 kill PID 23 with signal [15]: ,则继续按 Enter 保持默认设定即可。

4. 操作成功后,界面会出现 Send pid 23 signal [15/sigterm] 的提示信息,按 Enter 确认即可。

其它相关故障

CPU 空闲但高负载情况处理

问题描述

Load average 是 CPU 负载的评估,其值越高,说明其任务队列越长,处于等待执行的任务越多。 通过 top 观察,类似如下图所示,CPU 很空闲,但是 load average 却非常高。

top - 19:4	6:57 up 2	27 days,	5:33,	1 user,	load	average	e: 23,	22, 23	
Tasks: 94	total,	1 runni	ng, 93	sleeping,	0	stopped	d, O	zombie	
<pre>%Cpu(s):</pre>	0.3 us,	0.0 sy,	0.0 ni,	99.7 id,	0.0	wa, (0.0 hi,	0.0 si	i, 0.0 st
KiB Mem:	1016656	total,	950428	used,	66228	free,	1701	48 buffe	ers
KiB Swap:	0	total,	0	used,	0	free.	4527	40 cache	ed Mem

处理办法

执行以下命令,查看进程状态,并检查是否存在 D 状态进程。如下图所示:

ps -axjf

1	516	516	516	2	-1	Ss	0 0	:00	/sbin/iprinitdaemon
1	569	569	569	?	-1	Ss	0 0	:00	/sbin/iprdumpdaemon
1	863	863	863	?	-1	D+	38 0	:16	/usr/sbin/ntpd -u ntp:ntp -g
1	874	874	874	?	-1	Ss	0 0	:01	/usr/sbin/sshd -D
874	8823	8823	8823	2	-1	Ss	0 0	:03	_ sshd: root@pts/0
8823	8825	8825	8825	pts/0	9006	Ss	0 0	:00	\bash
8825	9006	9006	8825	pts/0	9006	D+	0 0	:00	_ps -axjf

() 说明

D 状态指不可中断的睡眠状态。该状态进程无法被杀死,也无法自行退出。

Г

· 若出现较多 D 状态进程,可通过恢复该进程依赖资源或重启系统进行解决。

swapd0 进程占用 CPU 较高处理

腾讯云

问题描述

Linux 系统通过分页机制管理内存的同时,将磁盘的一部分划出来作为虚拟内存。而 kswapd0 是 Linux 系统虚拟内存管理中负责换页的进程。当系统内存不足时,kswapd0 会频繁的进行换页操作。换页操作非常消耗 CPU 资源,导致该进程持续占用高 CPU 资源。

处理办法

1. 执行以下命令,找到 kswapd0 进程。

top			Б

2. 观察 kswapd0 进程状态。

若持续处于非睡眠状态,且运行时间较长并持续占用较高 CPU 资源,请执行如下 步骤3,查看内存的占用情况。

3. 执行 vmstat , free , ps 等指令,查询系统内进程的内存占用情况。 根据内存占用情况,重启系统或终止不需要且安全的进程。如果 si, so 的值也比较高,则表示系统存在频繁的换页操作,当前系统的物理内 存已经不能满足您的需要,请考虑升级系统内存。



云服务器实例无法登录

最近更新时间: 2023-02-23 11:18:23

简介

云服务器实例无法登录的故障原因有很多,其中腾讯云可观测平台可监控的故障包括云服务器带宽使用率过高和云服务器 CPU 或内存占用过 高。本文将为您介绍如何排查这两大故障原因。

故障原因

腾讯云可观测平台可监测无法登录云服务器实例的原因包括:

- 云服务器带宽使用率过高
- 云服务器 CPU 或内存占用过高

() 说明

在进行排查之前,需先排查是否因密码问题输入错误、忘记密码或者密码重置失败导致登录不成功。 可请参见 <u>重置实例密码</u> 重置实例密码。

处理步骤

云服务器带宽使用率过高

故障现象:通过自助诊断工具诊断,提示问题为带宽使用率过高。 处理步骤:

- 1. 通过 VNC 方式登录实例。
- 使用 VNC 登录 Windows 实例
- 使用 VNC 登录 Linux 实例
- 2. 参见 云服务器带宽使用率过高,查看实例的带宽使用情况和处理故障。

云服务器 CPU 或内存占用过高

故障现象:通过自助检查工具或者腾讯云可观测平台,显示云服务器 CPU或内存占用过高导致系统无法进行远程连接或者访问非常卡。 **可能原因**:病毒木马、第三方杀毒软件、应用程序异常、驱动异常或者软件后台的自动更新,会造成 CPU 占用率高,导致登录不上云服务器或 者访问慢的问题。

处理步骤:

- 1. 通过 VNC 方式登录实例。
- 使用 VNC 登录 Windows 实例
- 使用 VNC 登录 Linux 实例
- 2. 参见 云服务器 CPU 或内存占用过高,在 "任务管理器" 中定位高负载的进程。

() 说明

导致云服务器 实例无法登录的故障原因有很多,其它原因需请参见云服务器 无法登录 Windows 实例 或 无法登录 Linux 实例 文档 进行排查。



云服务器带宽使用率过高

最近更新时间: 2022-04-28 20:27:55

简介

本文档介绍因带宽占用高导致无法登录 Windows 和 Linux 云服务器实例的排查方法和解决方案。

故障定位及处理

- 1. 登录 云服务器控制台。
- 2. 选择待检查的云服务器,单击**登录**。如下图所示:

实例													实例使用指南 12
广州(6) • 上海(0)	北京(0)	成都(1)* 重度	(1) 中国香港(0)	新加坡(0)	曼谷(0)	孟买(0)	首尔(0)	东亰(0)	硅谷(0)	弗吉尼亚(0)	多伦多(0)	法兰壳福(0)	莫斯科(0)
新建 开机 关 所属项目:全部项目 关键字用	机 国 11分隔,过滤	E启 续费 // / / / / / / / / / / / / / / / / /	重置密码更多	桑作 ▼					Q	查看待回收实例			¢ ¢ ∓
ID/实例名	监控	状态 ▼	主机类型 ▼	主IP地址	ŧ		实例计费模式 `	r	网络	计费模式	換	作	
- Marco	di	也运行中	标准型S2 👬	11	(公) (内)		包年包月 4天后到期		按带	宽包年包月计费		读 读费 更多 ▼	
- J 25	di	⇒运行中	标准型S2		(弹性) (内)		包年包月 2019-09-26 14:23到期		按带	宽包年包月计费	ŝ	读 续费 更多 ▼	

- 3. 在弹出的 "登录Windows/Linux实例" 窗口中,选择**其它方式(VNC)**,单击**立即登录**,登录云服务器。
- 4. 在弹出的登录窗口中,选择左上角的 "发送远程命令",单击 Ctrl-Alt-Delete 进入系统登录界面。如下图所示:

发送远程命令 🔺	连接成功。如需粘贴命令,请点击 <u>这里</u>
<u>Ctrl-Alt-Delete</u>	
Ctrl-Alt-Backspace	
Ctrl-Alt-F1	按 Ctrl + Alt + Delete 登录。
Ctrl-Alt-F2	

针对 Windows 服务器

通过 VNC 方式登录 Windows 云服务器之后,您需要执行以下操作:



2. 选择**性能**页签,单击**打开资源监视器**。如下图所示:



r⊇	任务管理器	_ 🗆 X
文件(F)选项(O) 查看(V)		
进程 性能 用户 详细信息 服务		
CPU 39% 2.49 GHz	CPU Intel(R) Xeon	(R) Gold 61xx CPU
〇 内存 0.6/2.0 GB (30%)		
○ 磁盘 0 (C:) 读取: 20.5 KB/秒 写入: 12.4 M	60秒	
 以太网 发送: 40.0 Kbps 接收: 16.0 Kb 	利用率 速度 最大速度: 2 39% 2.49 GHz 插槽: 7	2.49 GHz
	送程 线程 句柄 虚拟机: 39 432 11429 L1 缓存: 2 援行: 2 援行: 2 成本 (11429) L1 緩存: 2 成本 (11429) L1 煖香(11429) L1 煖б(11429) L1 煖б(11429) L1 煖б(11429) L1 𝔅 (11429) L1 𝔅 (11429	I
	正常运行时间 0:00:12:42	
	7	~
◇ 简略信息(D) ◎ 打开资源监视器	Transa	

3. 在打开的 "资源监视器"中,查看消耗带宽较多的进程,并根据您的实际业务,判断此进程是否正常。如下图所示:

8			资	原监视器				_ 0 ×
文件(F) 监视器(M) 帮助(H) 概述 CPU 内存 磁盘	t 网络							
CPU 📕 4	% CPU 使	用率	100%	最大频率				~ 视图 ▼]^
磁盘 ■ □	千字节/秒	磁盘 I/O	📕 0% 最	长活动时间			CPU	100% -
网络 ■ 0	Kbps 网络	ł I/O	📕 0% 🎮	络使用率	Č			
名称	PID	地址	发送(字节	接收(字节	总数(字节	~		
svchost.exe (termsvcs)	1244	84.201.15	113	107	220			
BaradAgent.exe	1308	169.254.0.4	138	47	185			
svchost.exe (termsvcs)	1244	155.27.23	85	81	165	=	60秒	L %0
svchost.exe (termsvcs)	1244	92.119.16	90	65	155	-	磁盘	100千字节/秒
svchost.exe (termsvcs)	1244	119.90.26	35	27	62			
YDLive.exe	2588	169.254.0	33	15	48			
YDService.exe	2520	169.254.0	26	21	47			
svchost.exe (NetworkService)	824	10_141_9	0	19	19	\checkmark		
内存	硬中断/秒		📕 29% į	已用物理内存				
							网络	100 Kbps
							内存	100 硬中断/秒 7 ~

• 如果消耗带宽较多的进程为业务进程,则需要分析是否由于访问量变化引起,是否需要优化空间或者 升级服务器配置。

 如果消耗带宽较多的进程为异常进程,可能是病毒或木马导致,您可以自行终止进程或者使用安全软件进行查杀,也可以对数据备份后,重装 系统。



▲ 注意

Windows 系统下很多病毒程序会伪装成系统进程,您可以通过**任务管理器 > 进程**中的进程信息来进行初步鉴别: 正常的系统进程都会有完整的签名以及介绍,并且多数位于 C:\Windows\System32 目录下。病毒程序名字可能同系统进程一 样,但缺少签名及描述,位置也会比较不寻常。

• 如果消耗带宽较多的进程为腾讯云组件进程,请提交工单联系我们进行进一步定位处理。

针对 Linux 服务器

通过 VNC 方式登录 Linux 云服务器之后,您需要执行以下操作:

() 说明 以下操作以 CentOS 7.6 系统的云服务器为例。

1. 执行以下命令,安装 iftop 工具(iftop 工具为 Linux 服务器下的流量监控小工具)。

yum install iftop -y
① 说明
如果是 Ubuntu 系统,请执行 apt-get install iftop -y 命令。
2. 执行以下命令,安装 lsof。

yum install lsof -y

3. 执行以下命令,运行 iftop。如下图所示:

iftop

U	

Б

	12.5K	Ь		25.0КЪ	37.5Kb	50.0Kb		62.5Kb
W1_2_14_centos W1_2_14_centos W1_2_14_centos W1_2_14_centos W1_2_14_centos W1_2_14_centos W1_2_14_centos W1_2_14_centos W1_2_14_centos W1_2_14_centos W1_2_14_centos				<pre><=</pre>			b 90b b 912b b 912b b 58b b 58b b 58b b 32b b 0b b 0b b 0b b 0b	78b 78b 987b 170b 29b 15b 8b 15b 8b 8b 8b
TX: RX: TOTAL:	cum: 69.4KB 42.1KB 111KB	peak:	6.82Kb 4.45Kb 11.3Kb			rates: 224 224 448	b 2.15Kb b 1.38Kb b 3.53Kb	2.26КЪ 1.37КЪ 3.63КЪ

• <= 、 => 表示流量的方向

TX 表示发送流量



Б

Б

- RX 表示接收流量
- TOTAL 表示总流量
- Cum 表示运行 iftop 到目前时间的总流量
- peak 表示流量峰值
- rates 分别表示过去2s、10s和40s的平均流量
- 4. 根据 iftop 中消耗流量的 IP,执行以下命令,查看连接该 IP 的进程。

lsof -i | grep IP

例如,消耗流量的 IP 为201.205.141.123,则执行以下命令:

lsof -i | grep 201.205.141.123

根据返回的如下结果,得知此服务器带宽主要由 SSH 进程消耗。

sshd 12145 root 3u IPV4 3294018 0t0 TCP 10.144.90.86:ssh->203.205.141.123:58614(ESTABLISHED) **D** sshd 12179 ubuntu 3u IPV4 3294018 0t0 TCP 10.144.90.86:ssh->203.205.141.123:58614(ESTABLISHED)

- 5. 查看消耗带宽的进程,判断此进程是否正常。
- 如果消耗带宽较多的进程为业务进程,则需要分析是否由于访问量变化引起,是否需要优化空间或者 升级服务器配置。
- 如果消耗带宽较多的进程为异常进程,可能是病毒或木马导致,您可以自行终止进程或者使用安全软件进行查杀,也可以对数据备份后,重装 系统。
- 如果消耗带宽较多的进程为腾讯云组件进程,请提交工单联系我们进行进一步定位处理。

建议您重点核查目的端 IP 归属地,可以通过 IP138查询网站 进行 IP 归属地查询。如果发现目的端 IP 归属地为国外,安全隐患更大,请务必重 点关注!



云服务器无监控数据

最近更新时间: 2023-01-31 12:08:21

简介

云服务器指标数据采集依赖于监控Agent。 若您没法正常获取监控指标数据,请参考本文排查故障。

建议您首先根据 安装监控组件 重新安装监控Agent,并等待3分钟查看监控数据是否恢复。若安装遇到问题或监控数据未恢复,请阅读下文详细 排查。

故障原因及处理方法

无监控数据原因	处理方法
未安装监控 Agent 或未启动 Agent	参见 步骤一 排查并处理故障
无法解析数据上报域名	参见 步骤二 排查并处理故障
Agent获取uuid错误	参见 步骤三 排查并处理故障
云服务器重启或关机	参见 步骤四 排查并处理故障
云服务器高负载	参见 步骤五 排查并处理故障

处理步骤

步骤一:检查是否安装监控组件 Agent 或是否启动 Agent

Linux 和 Windows 未安装监控 Agent 或未启动 Agent 的排查步骤不一致,详情请参见下文。





15286 pts/0 S+ 0:00 grepcolor=auto barad_agent 22515 ? S 0:06 barad_agent 22530 ? S 1:04 barad_agent 22531 ? Sl 10:16 barad_agent #若无显示或进程数量不符,则说明 Agent 异常,请以 root 账号执行以下命令启动 Agent ,提示 stargate agent run succ 和 barad_agent run succ ,表示重启成功。 cd /usr/local/qcloud/stargate/admin 「
若无显示或进程数量不符,则说明 Agent 异常,请以 root 账号执行以下命令启动 Agent ,提示 stargate agent run succ 和 barad_agent run succ ,表示重启成功。
cd /usr/local/qcloud/stargate/admin
cd /usr/local/qcloud/monitor/barad/admin
./stop.sh
./trystart.sh
① 说明
Agent启动后,等待3分钟后云服务器控制台确认是否已有监控数据。

步骤二:检查上报域名

监控 Agent 正常工作依赖下面 4 个域名正常解析:

- update2.agent.tencentyun.com
- receiver.barad.tencentyun.com
- custom.message.tencentyun.com
- metadata.tencentyun.com

Linux 和 Windows 检查上报域名和修复域名步骤不一致,详情请参见下文。

Linux Windows

1. 检查上报域名是否可以正常解析

执行下列命令,确认4个域名是否都能正常解析:

ping -c 1 update2.agent.tencentyun.com ping -c 1 receiver.barad.tencentyun.com ping -c 1 custom.message.tencentyun.com ping -c 1 metadata.tencentyun.com

正常情况下,在云服务器上可以正常解析以上4个域名,若上面的命令提示 unknown host 则表示域名无法解析,参见下列的方式修 复。

2. 修复域名解析

腾讯云在不同地域均提供了可靠的内网 DNS 服务器,建议不要覆盖默认 DNS 配置。如果需要修改默认 DNS 配置,可以参见以下方式修 复上述 4 个域名的解析问题。

2.1 如果使用自建 DNS 服务或第三方 DNS 服务,建议在 /etc/resolv.conf 中追加腾讯云提供的内网DNS,具体请参见 云服务器 内网 DNS列表

IP

2.2 如果使用自建 DNS,也可以把以上4个域名加到自建 DNS 中,域名和对应解析 IP 如下:

域名

Б



Б

update2.agent.tencentyun.com	169.254.0.15
receiver.barad.tencentyun.com	169.254.0.4
custom.message.tencentyun.com	169.254.0.5
metadata.tencentyun.com	169.254.0.23

3. 如果以上两个方式不可行,可以在服务器的 /etc/hosts 文件中增加如下配置:

169.254.0.15 update2.agent.tencentyun.com 169.254.0.4 receiver.barad.tencentyun.com 169.254.0.5 custom.message.tencentyun.com

169.254.0.23 metadata.tencentyun.com

🕛 说明

修复后,再次检查域名解析是否正常。域名解析正常后,等待3分钟后到云服务器控制台确认是否已有监控数据。

步骤三: 检查 uuid 是否正确

目前只有 Linux 会出现 uuid 配置不正确问题,详情请参见下文。

1. 进入 云服务器控制台 ,进入实例详情查看 uuid 。

← (main an	(as	\$-深圳业务)		
基本信息	弹性网卡	公网IP	监控	安全组
实例信息				
名称	as-深圳业务 🖍			
实例ID				
UUID	-4	c43-b49a-55df8	32342c20 🗖	
实例规格	标准型S5 S5.SM	IALL2		

2. 登录云服务器,执行以下命令查看 uuid 。





echo`cat /etc/uuid |awk -F '= ' '{print \$NF}'` > /etc/uuid_to_serial; mount --bind /etc/uuid_to_serial
/sys/class/dmi/id/product_serial
cd /usr/local/qcloud/stargate/admin
./restart.sh
cd /usr/local/qcloud/monitor/barad/admin
./stop.sh

./trystart.sh

() 说明

修复后,等待3分钟,然后到云服务器控制台确认是否已有监控数据。

步骤四:检查云服务器操作日志

云服务器操作关机后处于关机状态,会导致监控组件离线并且没有数据。

用户通过云服务器控制台或者登录云服务器,操作重启,升级云服务器,重装,制作镜像等常见的云服务器运维操作,都会使云服务器监控数据 上报超时导致离线。

问题排查方式:可以根据当时时间点排查云服务器是否有存在相关的运维操作,操作日志可以进入云服务器详情页面中操作日志中查看。

← management (m. cm)					登录 更多操作 ▼
基本信息 弹性网卡 公网IP	监控 安全组 操作	日志			
今天 近7天 近15天	近30天 2021-02-09~2021-03	-10			
操作时间	操作名称	Action	操作者	操作结果	详情
2021-03-10 15:14:55	关闭云主机V3	StopInstances	root	成功	洋情 🖸
2021-03-09 15:35:53	修改实例密码V3	ResetInstancesPassword	root	成功	详情 🖸

步骤五:检查云服务器负载

云服务器 CPU 高负载,内存使用占满,带宽占用过高都会导致监控组件上报数据异常。

问题排查方式:

- CPU 高负载:详细排查步骤请查看 云服务器 CPU 或内存占用过高。
- 内存占用过高:可以登录云服务器或者查看监控图表是否有存在内存使用达到 100% 的情况,若达到 100%,可以根据实际情况来扩容 服务。
- 带宽占用过高:详细排查步骤请查看 云服务器带宽使用率过高。



未收到告警

最近更新时间: 2023-02-23 11:18:24

本文档为您介绍未收到告警的排查方法和解决方案。

未收到告警原因

未收到告警原因	解决方法
告警策略未启用	参见 排查步骤一 开启告警策略
短信配额不足	参见 排查步骤二 排查并购买短信
未配置或未验证告曹通知渠道	参见 排查步骤三 排查并开启或验证告警渠道
接收组未配置用户	参见 排查步骤四 排查并配置用户
取关微信公众号	参见 排查步骤五 排查并关注公众号
未达到告警触发条件	参见 排查步骤六 排查并确认是否达到告警触发条件

排查步骤

步骤一: 查看告警策略是否启用

1. 进入 腾讯云可观测平台—告警策略。

- 2. 查看对应的告警策略是否开启。
- 如下图策略1,告警启停按钮为灰色则说明未开启告警策略,单击灰色按钮 > 确认开启即可。
- 如下图策略2,告警启停按钮为蓝色则说明告警策略已开启,请按照其它步骤继续排查。

策略名称	触发条件	所属项目 ▼	策略类型	已启用/实例数	最后修改 🛊	告警渠道	告警启停 ▼	操作
□ 策略1	磁盘利用率 > 70 内存利用率 > 90 CPU利用率 > 80	默认项目	云服务器-基础监	1/1	100013529809 2020/08/13 20:01:	接收组: 1个 有效期: 00:00:00 - 2: 渠道: 邮件、短信		· 复制删除
□ 策略2	CPU利用率 > 0%	默认项目	云数据库-MySQL	0/0	100015073240 2020/08/13 17:31:	接收组: 1个 有效期: 00:00:00 - 2: 渠道: 邮件、短信		复制删除

步骤二: 查看短信配额是否使用完

- 1. 进入 腾讯云可观测平台—告警历史 。
- 2.查看您的短信配额是否已使用完。

如下图显示 "剩余 0 条可用" ,则说明 "基础告警" 短信已使用完。每个告警类型、每用户、每月为1000条免费配额,若超过额度需继续



使用短信告警,请单击**购买短信**进行短信增量。

告警历史 基础告警 自定义告警							告警策略使用打	晋引 🖸
● 当月短信配额已用 1000 条,	剩余 0 条可用。购买短信							
今天 昨天 近7天 发生时间 ↓	近30天 2020-08 告警对象 告警内容	-17~2020-08-17 📩	告警状态 ▼	结束时间	告察类型	请输入告警对象 	Q 文 洛称	± 🕢
2020/08/17 21:44:00	CPU利…	21小时2 微信、邮件	未恢复	-	指标	云服务器-基础监控… test	告警 \	/PC
2020/08/17 21:43:00	. CPU利	21小时2 邮件、短信	未恢复	-	指标	云服务器-基础监控… test	当警 V	/PC

🕛 说明

如需了解短信收费详细说明,请参考 购买指南-短信配额 。

步骤三: 查看告警渠道是否配置/验证

- 1. 登录 访问管理控制台。
- 2. 在用户列表中单击对应的用户名称,进入用户详情页。

	子用户			
账号ID	100 98	手机	- /	
备注	-	邮箱	- /	
访问方式 🛈	控制台访问	微信		
		是否允许微信接收通知	否	

• 告警渠道未验证: 如下图所示则说明告警渠道未验证,请单击认证。

← 用户详情			
test2 子用户			编辑信息
账号ID	手机	发送验证链接	
备注 -	邮箱	发送验证链接	
访问方式 ① 控制台访问	微信	-	
	是否允许微信接收通知	是(未验证) 发送验证链接 [●]	

发送成功后请前往各渠道进行认证。

- 短信认证:请前往您的手机短信单击相关链接进行认证。
- 邮箱认证:请登录您的邮箱单击相关链接进行认证。



• 微信认证: 请参见 微信渠道 进行认证。

步骤四: 查看告警接收组是否配置用户

- 1. 进入 腾讯云可观测平台—告警策略。
- 2. 找到对应的告警策略,单击策略名称,进入告警策略管理页。
- 3. 查看告警接收对象是否包含未收到告警的用户。若出现"未设置"或没有此用户,请参考创建告警接收组添加用户到告警接收组。

告警接收对象				
编辑 解除				
接收组	接收人	有效时段	告警渠道	操作
test-gary	未设置	00:00:00 - 23:59:59	邮件、短信	解除

步骤五: 查看是否取关微信公众号

() 说明

进行此步骤前请确保您的微信渠道是否认证,如未认证请参考 微信渠道 进行认证。

您可以用微信扫下列二维码查看是否已取消关注"腾讯云助手"公众号。



若出现"关注公众号"按钮则说明已取消关注。请重新单击**关注公众号**,才能正常接收微信告警通知。



步骤六: 查看是否达到告警触发条件

查看指标告警是否到达触发条件

例如:设置指标为 CPU 利用率 、比较关系为 > 、阈值为80% 、统计粒度为5分钟 、持续周期为2个周期。 表示:每5分钟收集一次 CPU 利用 率数据,若某台云服务器的 CPU 利用率**连续两次**大于80%则触发告警。 以此类推,设置持续周期为 N,则需要指标监控数据 N 次达到阈值才 会产生告警。

您可以登录 腾讯云可观测平台,选择对应的云产品,单击 ^山 查看指标监控数据,通过时间筛选器确认指标监控数据是否达到触发告警条件,未 达到则不发送告警通知。



如下图所示:查看云服务器 CPU 利用率。

云监控	HOT 推广新客上云即可获赚积分,推广新香萄多积分越多。最高可兑换10万元无门	(多实例对比监控 C 设置告答 C)
IEI 해서:++\/D ~	云服务器-基础监控 广州(5)[●] 上海(1) 南京 北京 成都 重庆	長 実財 近24小时 近7天 法择日期 薗 时间胞度 10秒 ▼ ◇
		CPU 内存 内网带宽 外网带宽 磁盘使用 分区使用情况
(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	健康状态: 异常(2)提醒(0)	
		CPU CPU利用率 40 -
四 流量监控	<u>实时</u> 近24小时 近7天 选择日期 節	*© 20 - 0 - with mouth with the stand with the stan
☞ 黑石网络监控	ID/主机名 监控 状态 网络类型 IP地址	基础CPU使用家 40 -
云产品监控	山 运行中 VPC 网络	* 0 20 20
◎ 云服务器		1000 -
四 块存储	II 运行中 VPC 网络	内存 内存使用量 MB① 500 -
Ei 负载均衡-CLB		0 -