



阿里云公共DNS 控制台操作指南

文档版本: 20210628



法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。 如果您阅读或使用本文档,您的阅读或使用行为将被视为对本声明全部内容的认可。

- 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档,且仅能用 于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息,您应当严格 遵守保密义务;未经阿里云事先书面同意,您不得向任何第三方披露本手册内容或 提供给任何第三方使用。
- 未经阿里云事先书面许可,任何单位、公司或个人不得擅自摘抄、翻译、复制本文 档内容的部分或全部,不得以任何方式或途径进行传播和宣传。
- 由于产品版本升级、调整或其他原因,本文档内容有可能变更。阿里云保留在没有 任何通知或者提示下对本文档的内容进行修改的权利,并在阿里云授权通道中不时 发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠 道下载、获取最新版的用户文档。
- 4. 本文档仅作为用户使用阿里云产品及服务的参考性指引,阿里云以产品及服务的"现状"、"有缺陷"和"当前功能"的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引,但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的,阿里云不承担任何法律责任。在任何情况下,阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害,包括用户使用或信赖本文档而遭受的利润损失,承担责任(即使阿里云已被告知该等损失的可能性)。
- 5. 阿里云网站上所有内容,包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计,均由阿里云和/或其关联公司依法拥有其知识产权,包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意,任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外,未经阿里云事先书面同意,任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称(包括但不限于单独为或以组合形式包含"阿里云"、"Aliyun"、"万网"等阿里云和/或其关联公司品牌,上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司)。
- 6. 如若发现本文档存在任何错误,请与阿里云取得直接联系。

通用约定

格式	说明	样例
⚠ 危险	该类警示信息将导致系统重大变更甚至故 障,或者导致人身伤害等结果。	⚠ 危险 重置操作将丢失用户配置数据。
⚠ 警告	该类警示信息可能会导致系统重大变更甚 至故障,或者导致人身伤害等结果。	警告 重启操作将导致业务中断,恢复业务 时间约十分钟。
〔〕) 注意	用于警示信息、补充说明等,是用户必须 了解的内容。	大意 权重设置为0,该服务器不会再接受新 请求。
? 说明	用于补充说明、最佳实践、窍门等,不是 用户必须了解的内容。	⑦ 说明您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在 结果确认 页面,单击 确定 。
Courier字体	命令或代码。	执行 cd /d C:/window 命令,进入 Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid
[] 或者 [alb]	表示可选项,至多选择一个。	ipconfig [-all -t]
{} 或者 {a b}	表示必选项,至多选择一个。	switch {act ive st and}

目录

1.概览	05
2.域名列表	10
3.DNS防火墙	12
4.在线体验	15
5.计费数据	16
6.产品接入	17
7.产品鉴权	19
8.日志查询	20
9.SDK下载	21

1.概览

本章节将对公共DNS售卖版的控制台布局和概览页进行介绍。

控制台总览

公共DNS的控制台由以下六个模块组成

- 概览:对当前账号下接入公共DNS服务的概况进行介绍。包括整体概览和安全威胁概览,其中安全威胁概览仅限开通DNS防火墙功能的用户使用。
- 域名列表:列举出所选时间范围内有请求的域名和子域名的列表,以及其解析量的展示。
- DNS防火墙:对DNS访问请求中的木马、钓鱼等威胁进行检测和告警。目前仅对企业级用户开放。
- 在线体验: 在这个页面, 可以免费体验HTTP DNS的解析功能。
- 计费数据: 这个页面可以查看解析量、计费账单的情况。
- 更多: 更多菜单, 包括了产品鉴权配置、产品接入配置、以及日志查询的功能。

整体概览

整体概览分为三个部分。

概览	域名列表	DNS防火墙	在线体验	计费数据	更多					
整体概	览									安全威胁
近30	日接入情况概题	览② Acco	ount ID: 51280	[昨日威胁概	院				威肋等级: -
近30日 近30日	HTTP解析量: HTTPS解析量(含DoT/DoH) :	200 万次 0		远程控制	 新无数据 	^{木马} 0 0) 暫无数据	恶意软件 0	 新无数据
近30日 近30日	日接入域名数: 日威胁告警次数:		3.97 万个 -		挖矿 0	· ① 暂无数据		約 <u>鱼</u> 0	 新元数 	据
请求	星情况						昨天 ∨	2021-04-26	~ 202	I-04-26 🗒

第1部分:页面左侧的近30日内的接入流量情况

- Account ID: 根据阿里云账号自动生成, 是当前登录账号唯一绑定的ID;
- 近30日HTTP解析量:指您30日内的HTTP解析量统计,包括v4和v6的流量汇总;
- 近30日HTTPS解析量:公共DNS不单独统计DoH/DoT接入的流量,HTTPS解析量里包含了HTTPS、DoH、 DoT的流量汇总,包括v4和v6的总解析流量;
- 近30天接入域名数:指30日内有访问流量的接入的主域名数;
- 近30日威胁告警次数:指30日内所有威胁的总告警次数。

第2部分:页面右侧的昨日威胁概览(仅限开通DNS防火墙功能的用户查看)

右上角的威胁等级 A 高 是您昨日(如当前是4月10日11点05分,昨日指4月9日0-24点)发生的最高威胁等级;

远程控制、木马、恶意软件等缩略图能帮助您直观的看到昨日发生的威胁数量,以及威胁趋势。鼠标单击该 缩略图,能进入到 安全威胁 概览视图中查看详细的威胁报表情况。

第3部分:请求量情况

此处能查看最长90天内的公共DNS接入请求量情况。请根据您的实际接入情况,在HTTP/HTTPS,或者 TCP/UDP请求量里查看相关的请求量即可。







最下方是您活跃的域名和子域名的排名,按总请求量进行排名。总请求量指的是:HTTP+HTTPS(含 DoH/DoT)+TCP/UDP的请求量。单击"更多"可展示最大前100名的活跃域名/子域名信息,展开后的 TOP100排名里,能看到更细的v4和v6的解析量情况。

舌跃的	域名排名(单位:次)				活跃的]子域名排名(单位:次)			
排名	主域名	总请求量	HTTP请求量	HTTPS请求量	排名	子域名	总请求量	HTTP请求量	HTTPS请求量
1		3,326,662	0	0	1	':::" · · · et :	712,202	0	0
2	n	2,325,590	0	0	2	al al an	526,322	0	0
3	e com	1,220,885	0	0	3	ອະດີ	321,639	0	0
1	s	902,302	0	0	4	וראה הה הליליוי ירו	248,799	0	0
5		809,743	0	0	5	j i,i,)p i∋n ::	228,215	0	0
				更多					

如您接入了DNS防火墙功能,也能够看到威胁的域名/子域名排名。

威胁的	域名排名(单位:次)				威胁的]子域名排名(单位:次)			
排名	主域名	总请求量	HTTP/HTTPS总请求量	最高威胁等级	排名	子域名	总请求量	HTTP/HTTPS总请求量	最高威胁等级
1		100	0	🛕 高级	1	; Z	100	0	▲ 高级
2	aynano.tv	72	0	▲ 高級	2	nja promunitalynano.tV	72	0	▲ 高级
3	-iusinat an	14	0	▲ 高級	3	¹ .7(uning*.cz	14	0	▲ 高級
4	mc	8	0	🛕 高級	4	chebure.	8	0	▲ 高級
5	9.000000d	7	0	🛕 高級	5	$h_{i}: \dots : i_{i}: i_{i} \in \mathcal{A}$	7	0	🛕 高级
				更多					更多

安全威胁概览

威胁概览,仅对接入【DNS防火墙】功能的用户开放。威胁概览从威胁类型、威胁数量、威胁严重程度、威胁来源几个方面帮您了解内网存在的安全威胁。

一、威胁报表

默认展示的是昨日的威胁告警最高级别,您也可以切换到成自定义的时间段,最长支持90天内的威胁信息查询。

-威胁总数,指您当前出现威胁的数量总和;

-单击某一类威胁名称,如单击 🔽 远程控制: 66 💶 ,即只展示远程控制类型的威胁情况;

-根据威胁严重程度,每一类威胁类型都分为高、中、低三个类型;如 🗹 翰 : 3 🚥 🛛 三个颜色,分别代表

钓鱼类型的高、中、低,同一种类型的颜色越深,则威胁程度越严重。鼠标放在图片上时,能够看到每种威胁的高、中、低数量情况。

阿里云公共DNS



二、威胁事件

展示您查询时间段内的威胁事件情况,默认按威胁类型进行聚合,威胁严重的和总威胁请求量高的会靠前展示。

	威胁事件			威胁来源
帮助您了解访问过的哪些网站存在威胁。				
威胁等级 🔽	威胁类型	域名数量	请求量(次) 💠	最近威胁检测时间 🖕
+ 🛕 高级	恶意软件	9	66	2021-03-17 23:32:33
+ 🛕 高级	远程控制	10	66	2021-03-17 23:58:39

点击"+"号,能看到具体是哪些域名发生了威胁。威胁明细按威胁的请求量大小进行排序。

	威胁等级 🔽	威胁类型	域名数量	请求量(次) 👙	最近威胁检	测时间 🝦
-	▲ 高级	恶意软件	9	66	2021-03-	17 23:32:33
	威胁域名		最近威胁检测时间			请求量(次)
	.011		2021-03-17 23:32	33		41
	"n		2021-03-17 23:31:	59		15
	mc		2021-03-17 20:45	29		3
	аспіп.равна.соїї		2021-03-17 14:10:	51		2

三、威胁来源

此处展示您的威胁访问来源,能看到具体是哪些IP地址访问了威胁域名,以及访问了多少次。

	威胁事件				威胁来源	
展示TOP 100的威胁访问	可来源。					
					搜索访问源IP C	全部 ∨
访问源IP	威胁请求量 (次)	最高威胁等级	威胁类型	访问威胁域名数量 👙	最近威胁发现时间 🖕	操作
100.00.00	66	🛕 高级	恶意软件	9	2021-03-17 23:32:33	查看详情
	66	🛕 高级	远程控制	10	2021-03-17 23:58:39	查看详情





音看详情

2.域名列表

本章节详细介绍域名列表功能,在本页面您能参考域名和子域名的流量和威胁信息。

当您通过接入公共DNS之后,您可以在域名列表这里看到所有有流量的域名信息。无需手动添加域名,90日 内有解析的域名都会智能展示在这里。

一、查看域名列表

云解析DNS / 公共DNS ⑦ 公共DNS产品简介 公共DNS 专注于对各种应用的互联终端,提供快速、安全、稳定的互联网连接方案。做好终端访问互联网的第一跳,使用前请先按要求接入公共DNS。接入说明 域名列表 DNS防火墙 在线体验 计费数据 概覧 更多 展示已接入系统的域名请求量信息,默认按所选时间的总请求量大小排序。 请输入要查找的域名 Q 2021-03-17 ~ 2021-03-17 域名名称 HTTP 解析量(次) HTTPS 解析量(次) UDP/TCP解析量(次) 威胁请求量 (次) 最高威胁等级 操作 0 0 1977381 查看详情

1381491

您可以查看不同协议(HTTP/HTTPS/UDP/TCP)的域名解析量情况,按所有类型的总解析量由大到小的顺序进行展示。其中DoH/DoT的流量包含在了HTTPS的解析量统计中。

如果您接入了【DNS防火墙】功能,则能看到威胁的展示情况,当主域名下存在多种威胁时,将展示最高的 威胁等级;

如果您有多个域名,可以通过右上角的搜索框进行模糊查询。如果查询的是子域名,则会默认匹配到其所在 的主域名。

二、查看域名的详细信息

0

找到关注的域名,在操作概览点击"详情",即可展开详细的域名解析量信息。

0

			请输入要查找的域名	٩	昨天 ~	2021-03-17 ~	2021-03-17	
域名名称	HTTP 解析量(次)	HTTPS 解析量(次)	UDP/TCP解析量(次)	威服	}请求量(次)	最高威胁等级	操作	
	0	0	1977381			-	查看详情	

当前域名下,90天内有访问流量的子域名都会集中显示在这里。您也可以通过搜索框,快速匹配到想查看的 子域名。

域名: n.com)
请输入要查找的子域名	Q		昨天 🗸	2021-03-17	~ 2021-03	-17 🛱
子域名名称	HTTP 解析量(次)	HTTPS 解析量(次)	UDP/TCP解析量(次)	威胁请求量(次)	访问源ip数	威胁情况
in.com	0	0	29174	0	1	-
	0	0	29025	0	1	2
cdn.com	0	0	28875	0	1	-
cdn.com	0	0	28832	0	1	-
, dn.com	0	0	28813	0	1	÷

单击子域名以后,解析量统计图会切换为您选中的子域名的解析量。



3.DNS防火墙

DNS防火墙功能仅面向企业认证的用户提供,目前公测阶段,在控制台提交申请以后就可以免费使用。公测 结束时间预计为12月31日,以页面具体通知为准。DNS防火墙公测申请

DNS防火墙配置

DNS防火墙是将DNS技术和安全威胁防护库相结合,从网络互联的入口处对域名请求进行威胁判断,选择性的对正常域名请求进行解析,阻止恶意域名解析和外联,从而保护企业内网安全的一种手段。

开通DNS防火墙功能后,即自动开启对以下类型的威胁访问检测:

威胁类型	描述
木马	发现存在木马病毒的网站,这类网站可能窃取用户信息及 破坏服务器文件。
钓鱼	发现用于窃取用户信息的欺诈性网站。
恶意软件	托管恶意内容的网站和其他受感染的网站。
远程控制	访问该网站可能泄漏用户信息或者导致网络中的其他设备 也受到感染。
挖矿	通过接管用户的计算资源来挖掘加密货币的网站

发现威胁以后的处置规则, 仅支持告警, 暂不支持阻断的方式。

云监控告警配置

在云监控中,对公共DNS的告警事件进行配置以后,您才能接收到公共DNS的告警信息。

- 1、打开云监控控制台
- 2、创建事件报警

-在云监控控制台的如下位置,选择**创建事件报警**

∃ (→)阿里云		Q 搜索文档、控制台、API、解决方案和资源 费用 工单 备案 企业	支持 App 🖾 🗘 📮 🕜 简体 🥘
云监控	事件监控		⑦ 快速入门 ⑦ 如何上报数据 ⑦ 最佳实践
概览 Dashboard ~	事件查询 报警规则		こ 刷新
应用分组	系统事件 目定义事件		
主机监控	请输入要查询的报警规则名称 搜索		创建事件报警
事件监控	规则名称 启用 规则描述	资源范围 目标	操作
自定义监控			
日志监控		目前还没有报警规则,您可以点击 这里 添加一个	
站点监控 🗸			
云产品监控			

-产品类型中,选中**公共DNS**

建/修以争件报音		
基本信息		
•报警规则名称		
公共DNS告警		
車件捉勶抑则		
事件类型		
 系统事件 自定义事件 		
产品类型		
公共DNS	•	
事件类型		
全部类型 🗙	•	
事件等级		
严重 ★	•	
事件名称		
全部事件 🗙		

-事件类型中,根据您的需求,选择需要告警的类型。

ᅔ	-	×	ŝ	刑	J.
		7	5	-	-

公共DNS	•
5件类型	
c&c 🗙	•
全部类型	
🗸 c&c	
cryptomining	
malware	
] phishing	
🗌 trojan	
确定 取消	

-配置好您定义的事件等级、报警方式。

报警方式

☑ 报警通知

联系人组	删除		
	•		
通知方式			
Warning (短信+邮箱+钉钉机器人)	•		

+添加操作

配置完成后,云监控的报警规则处就会生成一条公共DNS的告警规则。

关于云监控的事件报警规则,您可以参考<mark>云监控-创建事件报警规则,</mark>报警的联系人修改,请参考<mark>云监控报</mark> 警联系人操作。

3、查看云监控告警

您可以在云监控的事件查询里,看到公共DNS的告警信息。

4.在线体验

为了方便您快速试用公共DNS服务,我们在公共DNS控制台中增加了在线体验功能。

输入解析域名

您可以在「在线体验」页面中输入任意有效域名进行解析。

查看解析结果

输入域名后,点击「查询」按钮,即可查看解析结果。

公共DNS

专注于对	甘各种应用的互联	关终端,提供快速、	安全、稳定的五	互联网连接方案。	做好终端记	访问互联网的第一跳,使用前请先按要求接入公共DNS。 <mark>接入说</mark> 明
概览	域名列表	DNS防火墙	在线体验	计费数据	更多	
www.aliyun.com 查询						
地址类型			地址			归属地信息
IPV4				39		中国 上海市 阿里云

5.计费数据

公共DNS的计费数据页面,可以查看您的免费月解析量使用情况,以及最长90天内的HTTP/HTTPS解析量情况。

计费情况:

流量的抵扣顺序为:月免费流量-->资源流量包-->后付费流量。

默认展示昨日的解析量情况,您也可以通过切换自定义时间,查询指定时间内的解析量情况。

概览	域名列表	DNS防火墙	在线体验	计费数据	更多					
服务状态								本月剩余;	免费普通流雪	置 0
昨日》	流量统计				自定义时间流量统计	30天 ~	2021-02-16	~ 2021-03-	17 🛱	
昨日H 昨日H 昨日V	TTP解析量: 0 TTPS (含DoH/D DP/TCP解析量:	oT) 解析量: 22 1799.38 万次	次		30日HTTP解析量: 0 30日HTTPS(含DoH/DoT)解析量: 22次 30日UDP/TCP解析量: 1799.38万次					

公共DNS按日生成计费账单,详情费用情况您可以在费用中心查看。

停服:

如果您不想使用公共DNS服务,可以在这里手动停止服务。

服务状态

🗋 警告

请慎重操作停服功能。停服后将降级为免费用户,即停止计费、停止DNS防火墙功能及控制台的其他功 能操作和报表展示。您的公共DNS服务也将不再有SLA保证。

停服之后支持重启服务。重启后,服务恢复原来的配置,并重新开始计费。

6.产品接入

公共DNS售卖版支持HTTP/HTTPS、UDP/TCP的接入方式。您可以在【更多/产品接入】菜单里,找到本页面的入口。

HTTP/HTTPS接入

- 一、SDK接入
- 1、根据需要安装的操作系统,选择合适的安卓、iOS的SDK下载。
- 2、在您的APP上进行集成,可以参考
- Android SDK开发指南
- iOS SDK开发指南
- 3、集成完毕后,请在控制台概览页进行验证,有流量数据即为接入成功。
- 二、DoH JSON API调用

DoHJSON API的URL 接口 (提供TLS和非TLS API)

https://dns.alidns.com/resolve?

https://alidns_ip/resolve?

http://dns.alidns.com/resolve?

http://alidns_ip/resolve?

详情请查看DoH JSON API

三、DoT/DoH的接入方式

您可以按如下格式进行接入, user_id即为控制台上的Account ID。

DoT请配置: user_id.alidns.com

DoH请配置: https://user_id.alidns.com/dns-query?

- DoT接口的详细说明,请参考: DNS over TLS (DoT)
- DoH接口的详细说明,请参考: DNS over HTTPs(DoH)

DoT/DoH的接入开关:系统默认是关闭的,如需要DoH/DoT的接入,请手动打开。关闭状态时,DoH/DoT的流量接入会按免费版用户处理,即不提供SLA保证,也无法在控制台查看相关报表流量。

请注意: DoH/DoT不支持产品鉴权,有可能出现盗刷数据。如您需要接收DoH/DoT的流量,请手动开启。

UDP/TCP接入

注:此种接入方式,仅向企业认证的用户提供,个人用户不支持配置TCP/UDP接入。

请务必确定填写的IP地址,和您当前登录控制台的IP地址是一个,我们会对IP地址的归属进行校验。只有登录 控制台的IP地址和您填写接入的IP地址一致,并且该IP没有被别的用户占用,才能够接入成功。目前控制台只 支持单IP的接入方式。

接入状态解释:

接入状态	说明
已接入	您配置的IP地址已经正常接入公共DNS,并且系统判断最 近有来自于该IP地址的DNS请求。
已验证(不活跃)	您配置的IP地址已经过归属验证,但系统超过4小时未收 到来自该IP地址的请求。
验证失败	以下两种情况视为验证失败: 1、您配置的IP地址已经被别人占用; 2、您配置的IP地址,已经长时间(超过7日)未有流量。

系统暂不支持DHCP的IP接入方式,也不支持IP段的配置。

如果您需要接入IP段,请准备以下材料,提交工单系统审核:

1、提供IP段的归属证明材料;

2、提供企业电子执照和账号证明。

7.产品鉴权

开启产品鉴权以后,能对接入公共DNS的流量进行鉴权,避免被第三方或者未授权者盗用和查看。您可以在 【更多/产品鉴权】里找到本页面入口。

鉴权支持类型

支持JSON API和SDK接入的方式。

注意: 由于DoH/DoT的流量不支持鉴权,即使这里开启了鉴权功能,也无法对DoH/DoT流量进行鉴权判断。

鉴权说明

如下图所示,您可以在页面上创建AccessKey。

← 产品鉴权 ^{磁权开启后,将不支持DoH/DoT的}	赛入,只支持 JsonAPI和sdk 的接入方式	ς.					
开启證权,能保证用户解析数据等信息, 不被第三方未授权者盜用和宣看。 AccessKey 是您访问阿里云公共DNS API 的密钥,请您务必要善保管! 注: DoH/DoT流量不支持鉴权, 系统只支持JsonAPI氛IsdK的投入方式鉴权。							
			1	创建AccessKey			
AccessKey ID	AccessKey Secret	生成时间	状态	操作			
1000280	······· ©	2021-03-17 14:14:19		删除			

您可以最多创建5个AccessKey,最少保留一个。如果您需要查看AccessKey Secret,需要进行手机验证。手机号为您阿里云账号上绑定的默认手机。经过手机验证后,才可以正常查看AccessKey Secret。

状态开启时, 鉴权生效; 关闭时鉴权不生效。

API接口请参考:公共DNS鉴权接口

8.日志查询

您可以在【更多/日志查询】页面查看威胁日志和操作日志

威胁日志

最大存储7天的威胁日志,7天内的威胁情况,您都能查询出来。

← 产品日志

威胁日志	操作日調	5										
只存储7天(内的威胁日志											
威胁等级:	全部	威胁类型:	全部	\sim	访问源IP:	请输入访问源IP	٩	威胁域名:	请输入威胁域名	Q		
威胁发生时间	: 202	1-03-17 ~	2021-	03-18								
威胁等级			威胁类型			访问源IP		ì	威胁域名		威胁发生时间	

퀈	궀	

操作日志

您在公共DNS上的所有操作都会记录在操作日志,最大存储90日的操作日志。

操作日志的内容,您可以通过操作内容关键词,模糊查找出来。

← 产品日志

威胁日志 操作日期						
只存储90天内的操作日源	5.					
	操作行为:	全部 > 操作内容关键词:	操作内容 Q	操作时间: 2021-03-11	~ 2021-03-18	Ħ
操作时间 (UTC+8)	操作模块	操作内容			操作行为	
2021-03-17 11:47:29	产品接入-TCP/UDP 接	入 新增 1	, 状态:已接入, 不活	跃	增加	
2021-03-17 09:42:43	产品服务	开通公共I	DNS服务		增加	

9.SDK下载

平台支持的SDK接入,都将在本页面进行集中展示。

公共DNS



目前支持iOS和安卓的SDK接入,后续我们将提供更丰富的SDK。