

数据安全审计 快速入门





【版权声明】

©2013-2025 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或95716。



文档目录

 快速入门

 数据安全审计 SaaS 型

 操作指引

 Agent 部署

 数据安全审计传统型

 产品初始化

 控制台登录

 产品部署

 账户体系说明

 Agent 部署



快速入门 数据安全审计 SaaS 型 操作指引

最近更新时间: 2025-05-26 18:00:22

本文将为您介绍如何快速使用数据安全审计 SaaS 型。

前提条件

已购买 数据安全审计SaaS型。

步骤1:同步数据资产

1. 登录 数据安全审计控制台,单击侧边栏的数据资产,进入数据资产页面。

数据资产 ③ max ~							USRR*/SSRR*R	20/25 升级 区 操作指统				
	(銀库 (17) 白建数銀库 (4) 勝讯云外数)	盤峰 (3)										
○ 点が生きかべれたなどの表示があった。たらまではたがたないため、たままではただかたなどでは、つな方をごかななでは、、たままでのためでは、たまままでののでは、たまままでののでは、たまままでののでは、たまままでのでは、たまままでのでは、たまままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、まままでのでは、このでは、このでは、このでは、このでは、このでは、このでは、このでは、												
288/98 — — — — — — — — — — — — — — — — — — —	地球 ~					\$ †	XEFRER T 98. STERRE	artices Q D				
□ 第90/68 数据2*元型 数本	VPC	内側P	地域	就堂 点	公療主事计权限 罕	Agent@11608. V	CASSIFITER T	45				
4 MySQL 5.7			成都	夏 爾				63				
MySQL 8.0	11.070		重庆	28				63				
MySQL 8.0			R.R	28				63				
4 MySQL 5.7			RR	28				60				
MariaDB 8.0	a - 2010a		成都	28				60				
MyoaL 8.0			r.e	28				60				
MyoaL 8.0	a - 2010a		成都	28				600 C				
MyoaL 8.0	11.0755		#R	28				60				
MyoaL 8.0	10-1716F		EN	28				601				
MyoaL 8.0			r.e	28				601				
共 200 魚							10 ¥ ∰ / E H -	(1 /20)≣ ► н				

2. 通过单击更新资产列表拉取云数据库列表,也可使用自建数据库的添加数据资产功能,当需要审计腾讯云外的数据资产时,可在腾讯云外数据库添加。

3. 添加数据库后,可通过单击对应数据库后面的 🔵 ,开启审计权限,允许数据安全审计采集其日志进行安全分析。

数据资产 ③ 前級5 ~ 关系型云数据库 (173) NoSG	L云数据库 (55) 企业级分	や式云数据库(15) 自建	動還库(2) 商讯云外数据	库 (2)					已發稅资产/总接稅资产数 •	24/25 开级	CC HATTERN
通过更新资产列表起版合数的有利 并且立即生率计核和6、无数参考	O RUPERTWARKONNANNA, SURRUPERNANNANNANNANNANNANNANNANNANNANNANNANNAN										
	288807AU -	© зами -						81	X#7828 T 98, 5122	1.621月月午開分開	9.0
工程0/名称	發展资产类型	版本	VPC	15RP	1016	北西 〒	元原生每计纪题 Y	Agent@it628. T	CASB單计板用 Y	38-f7	
	MySQL	8.0			1813K	12				1211	
-	MySQL	8.0			лн	2.T				1211	
-	MySQL	6.7			12.40	ΞR				1911	
and the second second	MySQL	6.7			南京	28				1911	

△ 注意:

- 开启审计权限将消耗 License 授权资产数。
- 部分操作需要用户授权,只需按提示操作即可。
- 如果开启的是 CASB 审计权限,则需要购买 云访问安全代理,并且将对应元数据与代理绑定。

步骤2: 部署 Agent

1. 完成资产添加,并开启审计权限后,单击侧边栏的系统管理 > Agent 管理,进入 Agent 部署页面。



2. 在 Agent 部署中,根据数据库和应用系统所在位置和操作系统,下载对应的 Agent,进行部署。

Agenting © max -	C INTER
Agent## Agent#ist	
TRIBRANCTENERATE, BREACTING, BREACTING, BRANCES, BRANCESAN	
C 最高的Wegent	
这形于捕获2010年,或据过生结论拥获2010月前间每番,Agen和新起力非常是用一种形成推进合作进展。	
Linuquisme Linuquirant, geogenoculare,	
Uwuhhhili d. Yilkina Agart d. Yilkina Agart	
⑦ //####\$\$2, ###############################	
REERAAM	
ARTAINET-FOID-NERFORMERE BI TREA TO: AvvidEU.ORTERET-FORMER-FOR	
Linuezide## Linuedrt.htt, ##04905148##,	
Lundhald (1812.11) 4 182.co.days: 4 182.co.days:	

3. Agent 部署完成后,单击 Agent 列表,切换至 Agent 列表页面,验证 Agent 状态是否正常。

Agent管理 ⑤ #8区									CC Hoff Hold
Agent部署 Agent列表									
全部等着位置 *	© 2888 - 285	r v						10	ANTEPER Q
(FRP	部委位置	VPC	1814	操作系统	机动力和	最后上级时间	运行状态 〒	开启联告	26-17
10100-001	腾和四外			linus	CPU: 0% 内存: 0%	2024-11-13 14:57:54	· C商级		NOTE 10.01 (\$100)
	腾阳云内间		1°M	linus	CPU: 0% 内容: 0%	2024-10-09 15:34:02	· 巴肩线		5212 (0.0) (0.00)
	勝名四方國		I*M	linus	CPU: 0% P372: 0%	2023-08-13 09.03.55	· 已高级		5218 22-01 BHD
	勝限区外			windows	CPU: 0% P372: 0%	2024-04-01 17:07:56	· 已高级		STE 273 899
	勝限五内國		北京	linux	CPU: 0% PSW: 0%	2023-07-20 16:23:28	• 已易线		1248 1112 BRD
	勝刑元内阁		1°94	linux	CPU: 0% PNF: 0%	2023-07-20 1413:28	 已頁版 		1218 STR 802
具石垫								10 * 生/页	※ 4 1 /1賞 → K

步骤3:配置审计规则

开启数据资产的审计权限后,将默认启用常见内置审计规则。用户可在审计规则页面对规则进行进一步管理。

1. 单击侧边栏的安全运营 > 审计规则,进入规则列表页面,可查看系统中的审计规则,若内置规则无法满足您的特定需要,您可以单击新建创建自定义规则。

HARDI C DAK ~								co parte p
898 899							這種人類的名称	QD
##128	MROR V	NRINE V	MRE 7	用能等级 平	天政計畫资产	香油	80	
ExhereElisten I R	注观操作	内医规则	风险检测 (黑名章)	中风殿	20	操作规则	62.02	
60892 X X	注观操作	内医规则	风险检测 (黑名章)	中风殿	20	操作规则	610	
8.0845 (X) X	注观操作	内医规则	风险检测 (黑名章)	高风股	20	操作规则	4510	
BROUMPTLENS 2 2	数据地震	内医规则	风险检测(黑名章)	高风段	20	33822B	610	
8 X 488462X	注入政治	内医规则	风险检测(黑名章)	高风段	20	注入政告	6111	
WED-ELLX#P (\$ (\$	注入政治	内蓝戏剧	风险检测(黑名章)	高风段	20	注入政告	610	
MySQL-系统表型资用作2 常	违规操作	内蓝戏剧	风险检测(黑名章)	中风殿	19	操作发明	611	
MySQL-系统表型站器件1 常	违规操作	内蓝戏剧	风险检测 (景名章)	中风殿	19	操作发明	611	
MySQL-KULTHERT2 R	选现程作	内器放用	风险检测 (第名章)	4 8.8	19	制作发明	6250	
MySQL-XIER#128/P1 1	选现程作	内发放用	风险检测 (第名章)	4 8.8	19	操作规则	6240	
其741条							10~※/页 H 4 1 /7	531 F H

2. 单击规则启用,进入规则启用页面,选择数据资产,为其启用需要的审计规则。

ERI C name -						65 H
val v cn	01 1082				LIDIRA JUNI P	RER Q
100 20 10 10 10 10 10 10 10 10 10 10 10 10 10	無限分異 罕	MRMM T	植的装饰 Δ	网络琴根 丁	规则开关 罕	
DBMS_CDC_PUBLISHINEXTEND_WINDO	注入现面	内医规则	风险松湖 (第6年)	9R8		
XDB,RVTRIG,PKGMRVTRIG,UPD##59	注入观击	内置規則	网络松胡 (第65年)	9R.0		
金貨当菜用户校業 (OPMCLE装装)	法规操作	内置規則	网络松湖 (第65年)	9R.0		
朝用DEMS_METADATA的行为	法规操作	内置規則	风险检测 (第65年)	9R.0		
金粮GRACLE_SD	法规操作	内置規则	风险检测 (黑名甲)	與民族		
SQLServer-BATERER/METROP_MAKE	编制双击	内置規则	风险检测 (黑名甲)	15.04		
SQLServer-BATERER/MEDIREP_DROP	编和双击	内置規则	风险检测 (黑名甲)	98.M		
SQLServer-BATERER/MEDIREP_WLID	编和双击	内置規则	风险检测 (黑名甲)	98.M		
SQLServer-HittletightHittleSP_DROP	编程攻击	内五规则	风险检测 (黑名章)	98.0t		
SQLServer-执行危险的存储过程SP_SFAR	编程攻击	内五规则	风险检测 (黑名章)	98.M		
共741条					10 学 条 / 页 🖂 4 1	/7635 + +

步骤4: 查看审计日志



1. 完成以上配置后,在单击侧边栏的基础审计 > 审计日志,进入审计日志页面,可查看数据库的操作日志。

审计日志 审计日志	> 288 Q									C IANTAN
	Pe ~	2025-05-21-09:15:16 - 2	025-05-21 10:15:16	7.983 ·						± ≡
89	数据资产名称	用户名	客户場戸	明月 1	命中规则	波量來源 丫	风险等级 :	squilit(t)	847	
1	-			2025-06-21 10:11		7.898%	9 .9	SHOW	1996	
2	-			2025-05-21 10:10		7.838%	90 B	SHOW	1998	
э	-	-		2025-05-21 10:00	+	7.838%	89	22.1	1718	
4	-	-		2025-05-21 10:00	+	7.8385	89	1011	itta	
	-	-		2025-05-21 10:00	-	7.8385	安全	22.1	1718	
6	-	-		2025-05-21 10:00	-	28984	安全		1710	
7	-	-		2025-05-21 10:00	-	25965	安全		1710	
	-			2025-05-21 10:00	-	25965	安全	SET THE	1788	
9	-			2025-05-21 10:00	-	25965	安全	" and other an U.S. MPRC Real Andrews	1710	
10	-			2025-05-21 10:00	-	23965	安全	SET	1510	
共 44 首								10~余/页 H 4 1 3	/5)8 +	н

2. 单击侧边栏的**安全运营 > 风险识别**,进入 审计风险 页面,可查看发现的数据安全风险,安全管理人员可根据风险提示,判断是否需要采取进一步措施。

驗识别	~ 288 ©								
时民能	模型风险								
20000	r v	2025-05-20 00.00.00 -	2025-05-20 22.59:59 🗎	高量算法 •					
89	RHH# SB	用#8	8240	80R 1	命中规则	ilesi 7	RRWE :	SQL (84)	28-17
1	-		10.00	2025-05-20 17:20	XSINGRA	乙酰酮库	用风险	1 age of the line 111. Note that 411.	1718 1122.RH
2	-			2025-05-20 17:12	MyGQL-系统表面询操作1	राज्य	98.00	1 april 10 a	1718 BIRRN
а	-			2025-05-20 17:12	MyGQL-系统表面间操作1	乙酰酮库	98.00	1 Mart 10 Mart 10 Mart 11 Mart 10 Mart	1718 BIRRIN
4				2025-05-20 17:12	MyGGL-系统表面间操作1	त्तव	98.M	1 March 1997 (1997) (1997) (1997) (1997) (1997) (1997)	itte elsenate
5	-			2025-05-20 17:12	MyGQL-系统表面间操作1	rta	98.M	1 March 1999 (1999) (1999) (1997) (1997) (1997)	itin eliendi
6	-			2025-05-20 17:12	MyGQL-系统表型间操作1	四期前年	98.M	1 March 1999 (1999) (1999) (1997) (1997) (1997)	itin elikari
7	-			2025-05-20 17:12	MyGQL-系统表型间操作1	itiz	98.8	1 March 1999 (1999) (1999) (1997) (1997) (1997)	itin eliendi
	-			2025-05-20 17:12	MyGQL-系统表面间操作1	四期期時	98.8	1 Marco 1000 (1000 (111) - 8000) (1011) (101	itte exercit
9	-			2025-05-20 17:12	MyGQL-系统表面间操作1	元数据库	98.M	1 Marco Res (See 11) - Res (10) 101	ITH BURNES
10	-			2025-05-20 17:11	MyGQL-系统改变间接作1	rtut	QRAR	1 Marco 1000 (1000 (111) - 1000) (1010) (101	ITH BURNIN
共 156 余								10 ~ 条 / 页 H 4	/16页 H



Agent 部署

最近更新时间: 2025-05-26 18:00:22

概述

Agent 审计方式开启的全流程如下,其中"部署 Agent"指需部署 agent 到数据库服务器或访问数据库的应用服务器中,以确保可正常采集到数据库资产 的流量。

1. 配置数据资产实例并开启审计权限,操作详情请参见 管理数据资产。

2. 部署 Agent,支持在线部署或手动部署,操作详情请参见后文。

部署位置说明

根据所添加的数据库在云环境中的实际情况,您需要选择将 Agent 程序部署在以下位置:

- 自建数据库: Agent 程序需要部署在数据库所在的云服务器上。
- 云数据库: Agent 程序需要部署在对应的应用服务器上,通常为访问数据库的应用系统所在服务器。(如使用云原生审计方式,则无需部署agent)。

▲ 注意

- 腾讯云内网 Agent: 确保部署 Agent 的 VPC 已在 VPC 通道列表中,添加该 VPC 的资产即可自动创建 VPC 通道。
- 腾讯云外 Agent: 需要开通白名单,腾讯云外 Agent 才能正常上报流量。请 联系我们 协助开通。
- 在线部署 Agent: 需在线部署 Agent 的服务器,出方向需要放通端口443(下载 Agent 安装包)。
- 所有部署 Agent 的服务器,需要确保以下端口被开放:出方向需要放通端口8081(心跳通讯端口)、7000(日志采集流量通讯端口)、7001 (守护进程通信端口)。

部署操作

支持在线部署和手动部署两种方式,对于腾讯云内网服务器,推荐优先使用在线部署方式。

在线部署 Agent

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击 Agent 管理 > Agent 部署。
- 1. 在 Agent 部署页面,单击 Linux 在线部署。
- 2. 在 Agent 在线部署页面,选择 CVM 所在的地域和 VPC , 在需要部署 Agent 的 CVM 后单击**部署**,即可自动部署 Agent 。已经部署的 Agent ,可 执行卸载操作(即使 Agent 未连接,在此也可以在线卸载)。还可以选中多个 CVM ,进行批量部署。

△ 注意

- 在线部署暂时仅支持腾讯云内网的 Linux 操作系统。
- 使用在线部署的前提是该 CVM 实例已安装 自动化助手。



Agent在线部署						:	×
本功能仅支持已安装自动化助手,且处于在线	状态的云服务器CVM	٥					
北量部署・地域: 广州	▼ VPC:	请选择	•	请输入C	CVM IP/名称搜索	Q ¢)
实例ID/名称 VPC	地域	内网IP	操作系统 👅	自动化助手 👅	Agent状态 ▼	操作	
in	广州	1 :	Linux	未安装	• 未部署	部署	
int	广州	1	Linux	在线	• 未部署	部署	
in:	广州	1	Linux	在线	• 未部署	部署	
in	广州	1	Linux	在线	• 未部署	部署	
in:	广州	1 :	Linux	在线	• 未部署	部署	
共 0 条				10 ▼ 条/页 №	< 1 /	1页 🕨 🕅	

手动部署Agent

下载 Agent

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击 Agent 管理 > Agent 部署。
- 2. 在 Agent 部署页面,选择下载 Linux Agent 或 Windows Agent。

▲ 注意

- Agent 安装包已通过文件名区分部署场景,在部署前仔细检查,避免出错。
- 如 dsaagent_innernet_linux _xxx.zip 是腾讯云内网 Linux Agent。
- 如 dsaagent_outnet_win_xxx.zip 是腾讯云外 Windows Agent。

安装Agent

下载 Agent 完成后,需要将 Agent 安装在相应服务器上才能实现审计效果。

- 如果您使用的是云服务器 + 自建数据库模式,则建议您将 Agent 安装在数据库服务器上。
- 如果您使用的是云数据库,则需要在连接数据库的应用服务器上安装 Agent。

Linux 版本

△ 注意

Linux 需在部署 Agent 之前,安装Python 2.7运行环境。

1. 将 dsaagent_innernet_linux _xxx.zip 安装包上传到需要安装的机器上,如/data。

- 2. 使用 unzip dsaagent_innernet_xxx.zip 命令进行解压,得到 /data/CapAgent 目录。
- 3. 执行命令 chmod -R 755 CapAgent。
- 4.执行 cd CapAgent/bin ,再执行 nohup ./start.sh 1>/dev/null 2>/dev/nul 。
- 5. 在命令行,执行 netstat -ano | grep 7000 如下图即确认连接成功。

[root@VM-48-16-centos_dbAudit]# netstat -ano | grep 7000

tcp 0 0 FrontON 49 15 contac dbb		1	90	ESTABLISHED off (0.)
① 说明 其他命令。					
● 停止 agent:	nohup	./stop.sh	1>/dev/nu	ll 2>/dev/nul .	þ
● 重启 agent:	nohup	./restart.	sh 1>/dev,	/null 2>/dev/n	ul o



Windows 版本

- 数据安全审计 Agent Windows 版本只支持 Windows vista/2008 及以上版本。
- 1. 下载 Windows 版本 Agent 后,解压到安装目录。
- 2. 安装 Npcap。
 - 2.1 进入 CapAgent 下的 thirdparty 目录,双击 npcap-1.78.exe,单击 I Agree。

🗊 Npcap 1.78 Setup		_		\times
NMAP, ORG	License Agreement Please review the license term	s before installing	g Npcap 1.78	3.
Press Page Down to see th	e rest of the agreement.			
NPCAP COPYRIGHT / END	USER LICENSE AGREEMENT			^
Npcap (<u>https://npcap.com</u> library and is copyright (c) Project"). All rights reserv) is a Windows packet sniffing dri 2013-2023 by Nmap Software LL ed.	iver and LC ("The Nmap		
Even though Npcap source not open source software software without special p standard (free) version is	e code is publicly available for rev and may not be redistributed or ermission from the Nmap Project. usually limited to installation on fi	riew, it is used in other . The ve		÷
If you accept the terms of agreement to install Npcap	the agreement, click I Agree to c 1.78.	continue. You mus	t accept the	
Nullsoft Install System v3.07 -				
		I Agree	Can	cel

2.2 勾选 Install Npcap in WinPcap API-compatible Mode,单击 Install。

🗊 Npcap 1.78 Setup			—		\times
NMAP. ORG	Installation Opt Please review th	ions e following options	s before installin	g Npcap 1	.78
Restrict Npcap drive	r's access to Admini	strators only			
Support raw 802.11	traffic (and monito	r mode) for wireles	s adapters		
Install Npcap in Winf	cap API-compatible	Mode			
Nullsoft Install System v3.07 -					
		< Back	Install	Cano	el

2.3 单击 Next > Finish, Npcap 安装成功。



Npcap 1.78 Setup Finished Thank you for installing Npcap	_		
Npcap has been installed on your computer. Click Finish to close this wizard.			
Nullsoft Install System v3.07	nish	Cano	el

- 3. 进入 CapAgent下的 bin 目录,使用管理员用户双击 start.bat 文件。
- 4. 执行成功后,Console 显示结果如下图所示。同时,可以在任务管理器中,看到 CapAgentForWin.exe 进程。

C:\Users\Administrator\Des [SC] CreateService SUCCESS	ktop\CapAyent-release\bin>start.bat
SERVICE_NAME: CapAgent	
TYPE	: 10 WIN32_OWN_PROCESS
STATE	: 4 RUNNING
	<pre><stoppable, accepts_shutdown="" not_pausable,=""></stoppable,></pre>
WIN32_EXIT_CODE	: 0 <0x0>
SERVICE_EXIT_CODE	: 0 <0x0>
CHECKPOINT	: 0×0
WAIT_HINT	: 0×0
PID	: 892
FLAGS	
SUCCESS: The scheduled tas	k "runtime_monitor" has successfully been created.

- 5. 检查 CapAgentForWin 是否成功启动并连接审计服务成功。
 - 5.1 在任务管理器中确认 CapAgentForWin 进程已运行。

№ 任务管理器				
文件(E) 选项(O) 查看(<u>v</u>)			
进程 性能 应用历史记录	灵 启动	用户	详细信息	服务
夕 物 ^	DID	₩ ★		
	FID	1/123		
ApplicationFrameH	18968	止仕	至行	
armsvc.exe	3616	正在	运行	
📧 audiodq.exe	4608	正在	运行	
CapAgentForWin.e	22304	正在	运行	

5.2 在 cmd 控制台,执行 netstat -ano | findstr 7000 ,如下图即确认连接成功。

D	:\DBAudi TCP	t\CapAgent\bi	n>netstat - ¦29 4	ano fi 2	indstr)0	ESTA	BLISHE	D 14972		
	 说明 如果 	CapAgentFor	Win 不能运行或	netst	at -an	.0	findstr	7000	命令执行不成功,	请 联系我	们获得支持。

6. Agent 停止。

在 CapAgent_win/bin 目录下双击 stop.bat 文件即可。



数据安全审计传统型 产品初始化

最近更新时间: 2025-01-10 19:17:22

购买数据安全审计传统型后,初次使用前,需要进行初始化操作。下面为您详细介绍如何初始化。

- 1. 登录 数据安全审计控制台。
- 2. 在数据安全审计传统型控制台,可以看到您已购买的数据安全审计实例,选择尚未初始化的数据安全审计实例,单击右侧初始化。

序号	系统实例名	地域	网络	IP地址	已购规格	购买时间	到期时间	状态	操作
1		-	-	-	高级版	2021-05-20	2021-07-20	未初始化	初始化 续费 升级
2		-	-	-	合规版	2021-05-19	2021-06-19	〇初始化进行中	

3. 在弹出的初始化窗口,选择与需要审计的数据库对应的地域和 VPC、子网。

() 说明

- 每套数据安全审计,仅支持审计同一 VPC,若您的数据库在不同 VPC 中,请购买多套数据库安全审计。
- 若需要在金融区中部署,请单击初始化窗口中的详情。

则名	cd					
民格	合规版		호(\$886)	(i) 202	1-6-18	
出现	-华南地区-	——华东;	8X	-华北地区-	西南	地区
	广州	上海	南京	北京	成都	重庆
属网络		基础网络	2、丽安中	清使用金融专订	8. 点击评节	↑了解更多。
石属网络 子网	详情区 VPC 请选择乐属 请选择您需要 请选择乐属	基础网络 私有网络 * 审计的数据3 网络子网 *	 高安平 高产所属的 	请使用金融专订 VPC网络	8、点齿弹性	17.所更多。



控制台登录

最近更新时间: 2025-01-10 19:17:22

购买数据安全审计传统型后,您可进入数据安全审计管理界面进行配置,下面将为您详细介绍如何进入管理页面。

- 1. 登录 数据安全审计控制台。
- 2. 在数据安全审计传统型控制台,可以看到您已购买的数据安全审计实例,选择任意数据安全审计实例,单击右侧管理。



3. 浏览器将弹出新窗口以显示数据安全审计登录界面。

0	数据安全审计	
请输入您的用户名		
请输入您的密码		
	登录	
本系统已支	诗IPV6,请使用chrome浏览器	

4. 在登录界面输入系统管理员账户 sysadmin 与密码(默认密码在购买时将通过站内信发送)进入管理界面,即可开始配置。

石态记讼时,可以联系我们进行讼时里直。

产品部署 账户体系说明

🕥 腾讯云

最近更新时间: 2022-11-17 15:28:05

数据安全审计为严格确保自身系统安全,防止单一管理员账号权力过大导致内部失控,提供了三权分立账户体系。该体系具备三类管理员:系统管理员、审计 管理员、操作审计员,三者相互制约,确保安全。每个管理员的职责和权限如下:

系统管理员

负责数据安全审计系统自身相关信息的查询以及自身相关功能的配置,具备其他账号的增删改权限,该角色内置账号 sysadmin。

审计管理员

负责数据安全审计业务,包括资源管理、规则配置、审计信息查询等,该角色内置账号 useradmin。

操作审计员

负责审计数据安全审计各管理员账号的操作,防止其他管理员滥用职权进行非法操作,该角色内置账号 sysaudit。

▲ 注意

上述账号默认密码将在购买后通过腾讯云站内信发送,请注意查收站内信消息。



Agent 部署

最近更新时间: 2025-05-26 18:00:22

数据安全审计部署的核心目标是把 Agent 安装到数据库服务器或访问数据库的应用服务器中,并且确保数据库服务器或访问数据库的应用服务器,与数据安 全审计的审计实例能实现网络连通。

Agent 部署流程如下图所示,其中前五步为参数配置操作:

配置数据资产实例 设置审计服务 IP	→ 设置连接端口 → 设置停止审计阈值	→ 下载 Agent 安装 Agent
--------------------	---------------------	---------------------

Agent 程序部署位置

根据所添加的数据库在云环境中的实际部署方式,您需要将 Agent 程序部署在以下位置:

- 云服务器自建数据库: Agent 程序需要部署在数据库所在的云服务器上。
- 云数据库: Agent 程序需要部署在对应的应用服务器上,通常为访问数据库的应用系统所在服务器。

配置数据资产

- 1. 已完成 控制台登录 操作后,通过 useradmin 账号登录数据安全审计管理页面(默认密码在购买时将通过站内信发送),在左侧导航中,选择数据资产
 与 Agent > 审计的数据资产,进入审计的数据资产页面。
- 2. 在审计的数据资产页面,单击添加数据资产,进入添加数据资产框,输入数据资产名称,选择数据资产类型和数据资产 IP 和 Port。
- 数据资产名称:数据库名称,必填140个字符内。
- 数据资产类型:数据库的类型。
- 数据资产 IP: 数据库服务器 IP 地址。
- Port:数据资产对应的端口。

添加数据资产	×
*数据资产名称: 请输入数据资产名称	
* 数据资产类型:	~
* 数据资产IP: * Port: 3	
取消	确定

3. 单击确定,提示添加成功。

4. Agent 下载。

4.1 以 useradmin 账号登录数据安全审计管理页面,在左侧导航栏中,选择数据资产与Agent > 审计用 Agent,即可进入Agent配置页面。

4.2 在审计用 Agent 页面,选择 Agent下载 > 添加,输入 Agent 名称,勾选对应的数据资产。单击确定即可。

4.3 配置成功后,可以下载选择下载 Linux Agent、下载 Windows Agent或 Linux 在线部署进行配置 Agent。

()	说明
----	----

- 设置停止审计阈值。若被审计数据库因性能导致濒临宕机,可以通过关闭更多服务和进程缓解宕机情况。您可以设置一个基于 CPU 与内存使用率的阈值,当被审计数据库超过阈值时,Agent 将发送告警信息并停止工作,缓解数据库的性能压力。
- 如您要求 Agent 任何情况都进行工作,可将负载检测开关关闭,Agent将持续审计数据。



Agent呂和に・						
自定义审计服务器地址	•					
₩计服务∰(P: •		1	Port: •			
5载检测:						
CPU利用率		%	内存利用調	E		%
制计的数据资产:*	進择數据资产 (2)		i	已选择的数据资产	(0/2)	
	water and the second second	99-187-20-22 4P-221	Q	数据资产名称	数据资产类	코
		MYSQL				
		MYSQL				
			**			

Agent 安装

下载 Agent 完成后,需要将 Agent 安装在相应服务器上才能实现审计效果。

- 如果您使用的是云服务器 + 自建数据库模式,则建议您将 Agent 安装在数据库服务器上。
- 如果您使用的是 TencentDB,则需要在连接数据库的应用服务器上安装 Agent。

部署前确认 Agent 部署的机器和审计服务网络是否连通,使用 telnet 审计服务 IP 7000 (审计服务 IP 为 Agent 配置时审计服务 分配的 IP),如下图 所示,表示网络已经连通,如有问题请 提<mark>交工单</mark> 联系我们。



Linux 版本

- 1. 将 CapAgent_xxx.zip 安装包上传到需要安装的机器上,如 /data 目录。
- 2. 使用 unzip CapAgent_xxx.zip 命令进行解压,得到 /data/CapAgent 目录。
- 3. 执行命令 chmod -R 755 CapAgent。
- 4. 执行 cd CapAgent/bin ,再执行 ./start.sh ,结果如下,如未得到以下结果,请 提交工单 联系我们。

```
Success Stop CapAgent
[root@VM_0_18_centos /data/CapAgent/bin]# ./start.sh
success start ../bin/CapAgent
success start
```

5. 在命令行,执行 netstat -ano | grep 7000 如下图即确认连接成功。

C:\Users\Administrator\Desktop\CapAgent_v	/in_1_1587440	471\CapAgent_	in\CapAgent
in\bin>netstat -ano ¦ findstr 7000			
TCP	7000	ESTABLISHED	3940
TCP	7000	ESTABLISHED	3940

Windows 版本

▲ 注意



数据安全审计 Agent Windows 版本只支持 Windows vista/2008 及以上版本。

1. 下载 Windows 版本 Agent 后,解压到安装目录,进入 "CapAgent/conf"目录,修改 config.ini 中 device 配置为本机访问数据库网卡的 IP(一般为内网 IP),如下图所示:



log=0

2. 进入 CapAgent_win 目录,执行文件夹中 AuditCapAgentSteup.exe 程序依次安装 Python3.8 环境、npcap0.9984、执行 CapAgent_win。

名称	修改日期	类型	大小
CapAgent_win	2020/4/21 9:18	文件夹	
AuditCapAgentSteup.exe	2020/4/21 9:18	应用程序	27,462 KB

2.1 安装 Python3.8 环境,单击**下一步**,选择 Python3.8 安装的位置,单击**安装**。



<u>I</u>nstall

< <u>B</u>ack

Cancel



3. 执行成功后,Console 显示结果如下图所示。同时,可以在任务管理器中,看到 CapAgentForWin.exe 进程。

C:\Users\Administrator\Des [SC] CreateService SUCCESS	kto	op∖∕	CapAgent-release\bin>start.bat
SERVICE_NAME: CapAgent			
TYPE		10	WIN32_OWN_PROCESS
STATE		4	RUNNING
			<pre><stoppable, accepts_shutdown="" not_pausable,=""></stoppable,></pre>
WIN32_EXIT_CODE		Ø	<0x0>
SERVICE_EXIT_CODE		Ø	<0×0>
CHECKPOINT		Øx	3
WAIT_HINT		Øx	3
PID		89:	2
FLAGS			
SUCCESS: The scheduled task	k '	'ru	ntime_monitor" has successfully been created.

- 4. 检查 CapAgent_win 成功启动并连接审计服务成功。
 - 在任务管理器中确认 CapAgent_win 进程已运行,

1 <u>2</u>			Ta
File Options View			
Processes Performance	Users	Details	Services
Name		PID	Status
BaradAgent.exe		1032	Running
CapAgentForWin.exe		3296	Running
CcSvcHst.exe		1352	Running
𝕑 ccSvcHst.exe		2664	Running
chrome.exe		4600	Running
Chrome.exe		4640	Running

○ 在 cmd 控制台,执行 netstat -ano | findstr 7000 ,如下图即确认连接成功。

C: Wsers Administrator Desktop CapAgent_wi	in_1_1587440	471 \CapAgent_w	in\CapAgent_
ICP ICP ICP	7000 7000	ESTABLISHED ESTABLISHED	3940 3940

5. Agent 停止。

在 CapAgent_win/bin 目录下执行 stop.bat 即可。