

数据安全审计 操作指南







【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

操作指南 数据安全审计SaaS型 权限管理 数据资产 审计日志 审计日志 审计会话 日志投递 日志管理 日志备份管理 日志脱敏 日志服务 CLS 风险识别 审计风险 模型风险 审计报表 审计规则 智能分析 告警管理 告警历史 告警设置 Agent 管理 网络管理 自审计 数据安全审计传统型 v5.1.0 系统管理 系统资源监控 用户管理 OTP 设置 告警设置 备份服务器设置 审计管理 安全审计与分析 审计数据 规则配置 审计报表 数据资产与 Agent 操作日志管理 v5.0.8 系统管理 系统资源监控 用户管理 OTP 设置 告警设置 时间服务器 备份服务器设置 审计管理 安全审计与分析 审计数据 规则配置



审计报表 数据资产与 Agent 配置管理 审计单元配置 访问源配置 部门业务配置 操作日志管理 v5.0.7 系统管理 系统资源监控 用户管理 OTP 设置 告警设置 时间服务器 备份服务器设置 审计管理 安全审计与分析 审计数据 规则配置 审计报表 数据资产与 Agent 配置管理 审计单元配置 访问源配置 部门业务配置 操作日志管理 v5.0.6 系统管理 系统资源监控 用户管理 OTP 设置 告警设置 时间服务器 备份服务器 审计管理 安全审计与分析 审计数据 规则配置 审计报表 数据资产与 Agent 配置管理 审计组配置 访问源配置 部门业务配置 操作日志管理 v5.0.5 系统管理 系统资源监控 用户管理 Agent 管理 Agent 配置 Agent 列表 时间服务器



 系统设置

 告警设置

 备份服务器

 OTP 设置

 审计管理

 审计配置

 审计配置

 审计配置

 审计配置

 审计犯题置

 审计记级器

 自定义报表

 操作日志管理



操作指南 数据安全审计SaaS型 权限管理

最近更新时间: 2024-05-24 17:32:21

数据安全审计产品基于访问管理(Cloud Access Management,CAM)进行访问权限的控制,为确保子用户正常操作和使用数据安全审计产品,本文提供 相关权限授予操作指引。

权限策略总览

策略名	描述	是否必选	说明
QcloudCamReadOnlyAcc ess	用户与权限(CAM)只读访问权限	是	角色授权相关权限
QcloudCDSFullAccess	数据安全审计(CDS)全读写访问权限		数据安全审计产品所有功能操作权限
QcloudCDSReadOnlyAcce ss	数据安全审计(CDS)只读访问权限	是(二选一)	数据安全审计产品只读与访问权限

操作步骤

- 1. 登录 访问管理控制台,在左侧导航栏中,单击**用户 > 用户列表**。
- 2. 在用户列表页面,找到目标子用户,单击**授权**。

新建用户 更多操作 ▼			搜索用户名/	D/SecretId/手机/邮箱/酱注(多关键词空格隔开) Q ↓ ↓
□ 用户名称 \$	用户类型 ▼	账号ID	创建时间 \$	关联信息	操作
•	主账号	1	10		授权 更多操作 ▼
•	子用户	1	j	-	授权更多操作 マ 🕑
已选 0 项, 共 2 项				20 - 条/页	н ч 1 /1页 н н

3. 在关联策略弹窗中,搜索需要授权的策略名并选中,单击确定即可。

×



关联策略

选择策略 (共 2 条)			已选择 2 条		
数据安全审计 (CDS)	O Q		策略名	策略类型	
策略名	策略类型 ▼		QcloudCamReadOnlyAccess	252.2.5 2/2 200	0
QcloudCDSFullAccess 数据安全审计(CDS)全读写访问权限	预设策略		用户与权限(CAM)只读访问权限	现以末町	0
QcloudCDSReadOnlyAccess 数据安全审计(CDS)只读访问权限	预设策略	↔	QcloudCDSFullAccess 数据安全审计(CDS)全读写访问权限	预设策略	۵
支持按住 shift 键进行多选	海 索		10 M		



数据资产

最近更新时间: 2025-05-06 17:06:32

管理云数据库

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击数据资产 > 关系型云数据库,进入关系型云数据库页面。
- 2. 在关系型云数据库页面,单击**更新资产列表**,自动拉取您在腾讯云账号内的关系型云数据库、NoSQL 云数据库、企业级分布式云数据库,同步成功则会在列 表显示。

数据资产 🕓 普通区	Ŧ									
关系型云数据库(109)	NoSQL	云数据库 (31)	企业级	分布式云数据。	车(7)	自建数据库 ()	2) 腾	讯云外数据库(0)	
 通过更新资产列表 开启云原生审计权 	立取云数据库列表, 限后,无需部署Age	也可使用自建数 ent即可实现审计项	据库的添加数据 力能;开启资产的	资产功能,当需要 的审计权限后,需	要审计腾讯云外 要部署Agent	的数据资产时,可 才能正常审计; 如题	「在腾讯云外数 果您开通了CA	据库添加。 SB实例,则可以开	启代理审计权限。	
更新资产列表	双向审计配置	全部数据资产	≏类型 ▼	🔇 全部地域	~					
3 选择—个实例。	单击审计权	限的	,即审计	H权限开启	成1九。切	关闭宙计#	7限、将	不面审计该	资产,也无法	查看这资产的审计日志。
0.217 1,200) MP - P				NPR (10		×1 , 07012	
	· © 2888 ·		000	bend	17.5 ×	空幕体定计研究 *	Anna(田)+67日 m	STREPHEN T SE, STEEL		
No.000 No.000<	✓ \$ 20000 × E [‡]	VPC	内RP	1016 @X	86 र • 87	公司生平计核果 T	Agent@it628 T	STREETER T SE. STREET	R0 R0 R0	
ND 87-974 NO-411-821 2.0013-824 X RO-/Site Bite 7-824 My02. My02.	▼ ② ±38404 ▼ 554 0.0 80	WPC	ńRP	ninia Marika Marika	状态 T ・ 正定 ・ 正定	□ 回生平计核规 T	Agent@it68 T	5-7-2487/8235 T Sel. 5-7-2238 CASE#IHER T	© Q ↓ ↓	
Data://wk Data://kl State://kl X 300-88 Base://kl Myccl. Myccl. Myccl. Myccl.	 ● 全部時代 ● 全部時代 ● 本 ●	INC	9RP	1998 南京 南京 广州	112 T - 112 - 112 - 112 - 112	二週生率计核規 Y	Agent@it608 r	STREFERENCE TOR. STREET	20000492052 Q 0 809 600 600 600	
PARTAN RAVION 200880740 XR0/68 BBS740 Mo02 MO02 MO02 MO02 MO02 MO02 MO02	* © 2880 * &* &0 &0 &0 &0 &0 &0 &0 &0 &0 &0	nec.	́лве	1018 東京 下州 成都	10.5 7 • 2.32 • 2.32 • 2.32 • 2.32	 二級生平計核策 Y 〇 ○ <l< td=""><td>Agent@3t608LT</td><td>STREET OR. STOCK</td><td>0 0 0 10 10 10 10 10 10 10 10 10 10 10 1</td><td></td></l<>	Agent@3t608LT	STREET OR. STOCK	0 0 0 10 10 10 10 10 10 10 10 10 10 10 1	
SEATURE SEATURE <t< th=""><th> C 23864 <lic 23864<="" li=""> <lic 23864<="" li=""> <lic 23864<="" li=""> <li< th=""><th>162</th><th>ńRP</th><th>1014 电容 电容 广外 风俗</th><th>7 233 211 - 212 213 213 213 213</th><th>2月25年11日第 F (1) (1) (1) (1) (1) (1) (1) (1)</th><th>Agent@11038 T</th><th></th><th>ETENVESIE C. C.</th><th></th></li<></lic></lic></lic></th></t<>	 C 23864 <lic 23864<="" li=""> <lic 23864<="" li=""> <lic 23864<="" li=""> <li< th=""><th>162</th><th>ńRP</th><th>1014 电容 电容 广外 风俗</th><th>7 233 211 - 212 213 213 213 213</th><th>2月25年11日第 F (1) (1) (1) (1) (1) (1) (1) (1)</th><th>Agent@11038 T</th><th></th><th>ETENVESIE C. C.</th><th></th></li<></lic></lic></lic>	162	ńRP	1014 电容 电容 广外 风俗	7 233 211 - 212 213 213 213 213	2月25年11日第 F (1) (1) (1) (1) (1) (1) (1) (1)	Agent@11038 T		ETENVESIE C. C.	
222740 5047423 22886745 20060740 886740 20060740 886740 4002 4002 4002 4002 4002 4002	* C 23464 * 50 60 60 57	MG	ARP	10年 年年 年年 11月 11月 11月 11月 11月 11月 11月 11月	7 33 88 - 88 88 - 88	2.82.571478 ¥	Agent@11008.*		ал () () () () () () () () () () () () ()	
222745 2282745 2282745 2282745 2282745 0 0 0 0 0 0 0 0 0 0 0 0 0 0	▼	WC		104 8.8 7 M 6.8	7 23 88 - 88 - 88 -	 記述生学时代表 * (*) (Agent@11608.v	Station T on State	алан ал	
2227年5 2004/03 2208/040 2004/05 BBEF/20 BBEF/20 0 M02 0 0 M02 0 0 M02 0 0 M02 0	C 1284 E	wc		ин Ал Ал ГН Ав	80 Y 400 400 400 400		Agentational v		A DE CONTRACTOR	
2000000 2000000 REV/RB BEF/RE MO2 MO2 MO2 MO2	0 0 2000 0 10 10 10 10 10 10 10 10 10 10 10 10 10	₩ 与耗 Licer	we nse 授权3	101 AR AR AR AR AR AR AR AR AR AR AR AR AR	80 Y 188 188 188 198		Agentifiction v		enter	
2252742 2252742 225242742 225242742 225242742 225242742 4002 4002 4002 4002 4002 4002 4002 4002 4002 4002	© 2000年 → 10 10 10 10 10 10 10 10 10 10	₩ 与耗 Licer	nse 授权者	^{∞∞} ^{∞∞} [™] 资产数。	80. V 1928 1928 1928 1928		AgentGittQE Y		¢ ₽ eventual eventua	
· 2008/02 2008/20 · 2008/20 · 2007/20 · 2007/20 · 2007/20 · 2007/20 · 2007/20 · 2007/20 · 2007/20 · 2008/20 ·	○ 6 2894 • 56 50 50 57	[™] ∮耗 Licer Þ授权,只	ase 授权 需按提示		867 988 988 988					

• 云原生审计权限无需安装 Agent 即可实现云原生审计功能,当前只支持云数据库 MySQL。

管理自建数据库

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击数据资产 > 自建数据库,进入自建数据库页面。
- 2. 在自建数据库页面,单击**添加数据资产**,弹出添加数据资产弹窗。

数据资产	●普通区 🔹			-		
关系型云数据属	E (109)	NoSQL云数据库 (31)	企业级分布式云数据库	: (7)	自建数据库 (2)	腾讯云外数据库 (0)
 通过更新 开启云原 	资产列表拉取云数 生审计权限后, 5	数据库列表,也可使用自建数据库的 无需部署Agent即可实现审计功能;	的添加数据资产功能,当需要 开启资产的审计权限后,需要	审计腾讯云约 要 部署Ag ent	外的数据资产时,可在腾讯云 t才能正常审计;如果您开通	5外数据库添加。 了CASB实例,则可以开启代理审计权限。
添加数据资	产双向	审计配置 全部数据资产类型	2 🔻 🔇 全部地域	v		



添加数据资产		×
* 添加方式:	O 选择CVM ○ 手动输入IP	
* 地域:	◎ 广州	~
VPC:	请选择	*
* CVM实例:	请选择	*
* 数据资产名称:	请输入	
* 操作系统:	请选择	*
* 数据资产类型:	请选择	*
数据库版本:	请选择	Ŧ
★ 端口:	请输入	
* 字符集:	请选择	Ŧ
双向审计		
提交并关	闭 提交并继续添加 取消	

3. 在添加数据资产弹窗中,配置相关参数,单击**提交并继续添加**可再次添加。

参数名称	描述
添加方式	根据实际需求选择 选择 CVM 或手动输入 IP。 • 选择 CVM: 部署在私有网络CVM上的资产。 • 手动输入 IP:通过专线等方式与私有网络打通的资产。
地域	支持广州、上海、南京、北京、成都、重庆。添加成功后,不可更改。
VPC	可选项,可通过选择资产所在 VPC ,缩小 CVM 实例查找范围。
CVM实例	选择自建数据库所在的CVM实例。
数据资产名称	自定义名称,在64个字符之内,不能重复。
操作系统	选择数据库所在的操作系统。
数据库资产类型及对 应版本	 MySQL: 5.1、5.2、5.3、5.4、5.5、5.6、5.7、8.0。 PostgreSQL: 9、10、11、12、13、14。 SQL Server: 2008、2012、2014、2016、2017、2019。 Oracle: 8i、9i、10g、llg、12c、18c、19c。 Redis: 所有版本都支持。 MongoDB: 2.x、3.x、4.x。 TDSQL-MySQL: 5.7、8.0、10.1。 MariarDB: 5.1、5.2、5.3、5.5、10.0、10.1、10.2、10.3、10.4、10.5、10.6。 Hive: 所有版本都支持。 HBase: 所有版本都支持。 TDSQL-C MySQL: 5.7、8.0。 DM: V7、V8。 KingbaseES: V8。 GaussDB: 200、300。



	 TIDB: 4.5、5.0、6.5。 OCEANBASE: 4.2。
端口	1-65535。
加密审计协议	仅当数据资产类型为 MySQL 或 MariaDB 时,此选项可见。开启此选项后,支持用户上传密钥文件,审计开启了 SSL 加密的数据库。详情请参见 配置参考。
密钥文件	上传密钥文件,大小限制在1MB 以内。
私钥密码	可选项,若密钥带有密码,请在此输入,限64字符以内。

4. 添加成功后可自行开启审计权限或修改取消审计权限。

管理腾讯云外数据库

1. 登录 数据安全审计控制台,在左侧导航栏中,单击数据资产 > 腾讯云外数据库,进入腾讯云外数据库页面。

	 说明 腾讯云外数据库,适合部署在友商云或 IDC,而没有通过专线等方式与私有网络打通,需要通过公网进行流量采集的资产。
2.	在腾讯云外数据库页面,单击 添加数据资产 ,弹出添加数据资产弹窗。
	数据资产
	⑦ 通过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,当需要审计器讯云外的数据资产时,可在据讯云外数据审添加, 开启云原生审计权限后,无需都署Agent即可实现审计功能,开启资产的审计权限后,需要器署Agent才能正常审计;如果您开通了CASB实例,则可以开启代理审计权限。
	添加数据资产 双向审计配置 全部数据资产类型 ▼

3. 在添加数据资产弹窗中,配置相关参数,单击确定完成添加。



添加数据资产	:	×
* 数据资产名称:	请输入	
* 操作系统:	请选择	r
* 数据资产类型:	MySQL *	,
数据库版本:	请选择	,
* IP:	请输入	
* 端口:	请输入	
* 字符集:	请选择	,
双向审计		
✓ 加密审计协议 🛈	配置参考	
* 密钥文件 点击上传 未 请上传正确的	E上传 I密钥文件,大小1MB以内	
私钥密码 请输入私钥	密码,无密码则为空	
	确定 取消	

参数名称	描述
数据资产名称	自定义名称,在64个字符之内,不能重复。
操作系统	选择数据库所在的操作系统。
数据库资产类型及 对应版本	 MySQL: 5.1、5.2、5.3、5.4、5.5、5.6、5.7、8.0。 PostgreSQL: 9、10、11、12、13、14。 SQL Server: 2008、2012、2014、2016、2017、2019。 Oracle: 8i、9i、10g、llg、12c、18c、19c。 Redis: 所有版本都支持。 MongoDB: 2.x、3.x、4.x。 TDSQL-MySQL: 5.7、8.0、10.1。 MariarDB: 5.1、5.2、5.3、5.5、10.0、10.1、10.2、10.3、10.4、10.5、10.6。 Hive: 所有版本都支持。 HBase: 所有版本都支持。 TDSQL-C MySQL: 5.7、8.0。 DM: V7、V8。 KingbaseES: V8。 GaussDB: 200、300。 TIDB: 4.5、5.0、6.5。 OCEANBASE: 4.2。
IP	根据实际需求输入所需 IP。
端口	1-65535。
加密审计协议	仅当数据资产类型为 MySQL 或 MariaDB 时,此选项可见。开启此选项后,支持用户上传密钥文件,审计开启了 SSL 加密



	的数据库。详情请参见 配置参考。
密钥文件	上传密钥文件,大小限制在1MB 以内。
私钥密码	可选项,若密钥带有密码,请在此输入,限64字符以内。

4. 选择一个实例,单击审计权限开关的 🔵 ,即审计权限开启成功。

双向审计配置

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**数据资产**,进入数据资产管理页面。
- 2. 选择需要配置**双向审计**的数据库资产,单击操作栏中的编辑,弹出双向审计配置弹窗。

ENROAR XADDER	全部数据资产类型 *	© 28884 -							关键字用装线 鬥 分隔,多个过渡每	自用的全体分解	Q Ø
采用0/8 株	鼓艇这个贝型	版本	WPC	内部中	1614	秋西 〒	云原生辛计权限 T	Agent@itREE T	CASE@11408 Y	31-17	
di-parajit/add, rad, in-	MySQL	80	wmail.1	1.01.0.0	南京	• 正常				3233	
18-18-00-00-000, No. 10-	MySQL	8.0	w	10.000.00.0000	奥克.	• 正常				89	
18-1000-0.000	MySQL	80	w-705x41	11.0.41.1.008	ГM .	• 正常				900 E	
despire/talitanees.	MySQL	5.7	an-disting	10,000,000	成都	• E R				604	

3. 在双向审计配置弹窗中,单击开启**双向审计**,并设置单 SQL 返回存储行数、单 SQL 返回存储空间。

双向审计配置		×
实例ID	and an input	
实例名称	007456312	
内网IP	172.27.3.47.3388	
双向审计 🛈		
* 单SQL返回存储行数	99 行	
* 单SQL返回存储空间	16 KB	
	靡定 取消	

4. 单击确定,即可开启成功。





审计日志 审计日志

最近更新时间:2025-05-26 18:00:22

审计日志从 SQL 语句的维度,帮您进行安全分析。

检索审计日志

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**基础审计 > 审计日志**。
- 2. 在审计日志页面,可根据具体数据资产名称检索,还可以按最近一小时、今天、昨天、本周、上周、本月、上月、近半年、自定义日期检索。

22520	r	2025-81-81 00 00 00 - 2025-01-31 23 59 59 📋 ХОШИХ -				+ =
89	888768	第三日 小田 小田 本田 小田 本田 丁田	法国来签 7	R8998 1	50L810	80
1		874 HXX	7.8E4	**	13	ana.
2		20054F101 < 0 > 20254F201 < 0 > B - 二 三 同 五 六 B - 二 三 回 五 六	7.8E4	**	201	ana.
3		29 30 31 1 2 3 4 26 27 28 29 30 31 1 5 5 7 9 9 90 11 2 3 4 5 5 7 9	1556	**	135	me
4		12 13 14 15 16 17 18 9 10 11 12 13 14 15	1824	92	810	area.
6		19 20 21 22 23 24 25 16 17 18 19 20 21 22 26 27 28 29 30 31 1 23 24 25 26 27 28 1	1884	92	36T	area.
		алты ас	18101	92	80.4	1792

如需对审计日志进行指定检索。单击高级筛选,可根据用户名、命中规则、风险等级、客户端 IP 、事件类型、表名、字段名等关键字,输入具体值,单击查询,即可查看相关信息。

288887	▼ 2825-01-01-00:00 0 - 2025-01-31 23 59 59 団 単級用品 へ					1 =
97.52	Water 🔹	886429	1.259 •	SessionId	188A	
80.52	338.2	BEEP	(2012)	80.86	清韻入	
根据在升	针对操作语句	86460	(RB).	8298860	信仰人	
1049(78)	INWARATE - INWARATE	8/18	R8A	SCRINE	(TBA)	
352161	1983	84014	1982	使用工具	WBA.	
皇守総則		88	1988.			
8818	全部 マ	788	R8A			
**	80					

查看审计日志

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击基础审计 > 审计日志。
- 2. 在审计日志页面的日志列表中,选择所需日志,单击**详情**,进入审计日志详情页面。

18-8	数避费产名称	Rea	8A98P	889.4	命中规则	月10日長 0	sqL谱句	操作
1				2022-01-05 17:13		<u>8</u> 2	connect	1218
2	1000	root	-	2022-01-06 17:13		10.0	logout	94 8



3. 在审计日志详情页面,可查看该条日志的基本信息、详细信息。

审计日志详情		×
基本信息		
操作语句	SET i 展开	
操作类型	SET	
事件类型	DML	
操作时间	2025-01-31 23:59:58	
SessionId		
命中规则	-	
风险等级	安全	
数据库类型	MYSQL	
数据库IP		
数据库用户		
客户端IP		
客户端MAC	-	
客户端主机名	CdbInterface	
详细信息		
数据库	-	
表名	-	
字段名	no	
影响行数	0	
执行时间	44 ms	
返回消息	-	
返回码	0	
包长度	124	
使用工具	-	1

下载审计日志

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击基础审计 > 审计日志。
- 2. 在审计日志页面,单击右侧的 上,进行审计日志的下载。

全部数据类	r -	2825-01-01 00:00:00 - 202	5-01-31 23 59:59 🛅	A683 -					⊥ ≡
18-0	BERASB	8148	8/120	RR s	8-91211	沈显宋逝 Y	RBNG +	50LBN	8.0
1		-	****	2525-01-31 23:59		2.820F	10	ΩT	1795
2		-	-	2025-01-31 23:59		元教室作	22	127	ang.
2		-	-	2025-01-31 23:59		元教授库	92	78	1745
4		-	-	2025-01-31 23:59			<u>92</u>	940	1745
•			-	2025-01-31 23:50		1.020	**	RT	ana -



3. 审计日志将根据当前筛选条件进行下载,单击确定。

确定要下载审计日志「	吗?	×
审计日志将根据当前筛选	5条件进行下载,下载完成后,可去下载任务列表	— 将文件导出
	确定取消	
击	务列表,查看并管理下载任务。	
○ 单击 导出 ,即可将任 ○ 单击 删除 ,经过二次	E务下载至本地。 R确认后,即可删除所选任务。	
▲ 注意: 日志每次最大可导	出1GB,已完成的任务仅保留一天,请及	时下载日志。
 注意: 日志每次最大可导 下载任务列表 	出1GB,已完成的任务仅保留一天,请及	时下载日志。
 注意: 日志每次最大可号 下载任务列表 dsau 	2出1GB,已完成的任务仅保留一天,请及 ^{59.csv}	时下载日志。
 注意: 日志每次最大可号 下载任务列表 dsauⁱ 文件大小: 658.9K 	建出1GB,已完成的任务仅保留一天,请及 ^{39.csv}	2时下载日志。
 注意: 日志每次最大可号 下载任务列表 dsau 文件大小: 658.9K 执行成功 	建出1GB,已完成的任务仅保留一天,请及 i9.csv	时下载日志。 导世
 注意: 日志每次最大可号 下载任务列表 はsau 文件大小: 658.9K 执行成功 2024-01-25 15:56:53 	建出1GB,已完成的任务仅保留一天,请及	找时下载日志。
 注意: 日志每次最大可号 下载任务列表 dsau 文件大小: 658.9K 执行成功 2024-01-25 15:56:53 dsa 	2出1GB,已完成的任务仅保留一天,请及 ^{39.csv}	b时下载日志。 导±
 注意: 日志每次最大可号 下载任务列表 はsau 文件大小: 658.9K 执行成功 2024-01-25 15:56:53 dsa 文件大小: 376.6K 	2出1GB,已完成的任务仅保留一天,请及 59.csv	2时下载日志。 导出

2024-01-25 15:56:41



审计会话

最近更新时间: 2025-05-26 18:00:22

审计会话从数据库连接会话的维度,帮您进行安全分析。

检索审计会话

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击基础审计 > 审计日志。
- 2. 在审计日志页面,单击**审计会话**。
- 3. 在审计会话页面,可根据具体数据资产名称检索,还可以按最近一小时、今天、昨天、本周、上周、本月、上月、近半年、自定义日期检索。

2002	ar -	2025-01-01 00 00 00 - 2025-01-31 23 59 59 📋 英雄雑誌 -							
184	BHR^88	総正一小村 今天 昨天 本府 上川 本府 上川 NATE 0750	8PMP	REAP	申计日志数	RP8	登录状态	HEREY	80
4			-	10100			4.82	元数据2	1245
2			ALC: 10.1			-	+ 1870)	7.88.804	and the
а		29 30 31 1 2 3 4 26 27 28 29 30 31 1 5 6 7 8 9 10 11 2 3 4 5 6 7 8	-			-	+ 18/20	7.01.024	1745
4		12 13 14 15 16 17 18 9 10 11 12 13 14 15 19 20 21 22 23 24 25 16 17 18 19 20 21 22 22					+ 1820	238304	016
6		28 27 28 29 30 31 23 24 25 26 27 28 1	-			-	182	1.01.001	1245
		алын не	-			-	• 16.0)	2.他现在	1245

4. 如需对审计会话进行指定检索。单击**高级筛选**,可根据用户名、命中规则、风险等级、客户端 IP 等关键字,输入具体值,单击**查询**,即可查看相关信息。

2002207	* 2025-0-0-00.00.00 - 2025-0-31.23.50.50 [] RUNA.*			
818	108A	87.84	INUA Boostoned	200.5
BHAP	258A	0.07480	48.488	8%A
2×86	金郎 ·			
£H	28			

查看数据详情

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击基础审计 > 审计日志。
- 2. 在审计日志页面,单击审计会话。
- 3. 在审计会话页面,可单击某条记录详情,进入审计会话详情页面。

数据资产名称	命这开始的问	6332739360	BOSEP .	数据成10	前计日间数	用户名	教授状态	1917
-	2022-01-06 19:20	2022-01-05 19:20			3		• 成功	3758
1000	2022-01-06 19:20			1000	1		+ 820	348
1000	2022-01-06 19:20				4		• (Q2)	1216

4. 在审计会话详情页面,可查看该条日志的详细信息。

审计会话详情		×
会话开始时间	01–31 23:59:58	
会话结束时间	01–31 23:59:58	
SessionId		
数据库	-	
数据库IP		
用户名		
登录状态	成功	
客户端IP		
审计日志数	-	



日志投递

最近更新时间:2025-05-26 18:00:22

前提条件

- 已开通日志投递功能,费用详情请参见 计费概述 。
- 已完成角色授权操作。
- 已购买腾讯云 消息队列 CKafka 实例,按照实际日志用量来配置 CKafka 实例的带宽规格。
- 支撑环境接入 CKafka 时需 提交工单。

配置日志投递

- 1. 登录 数据安全审计控制台,在左侧导航栏选择基础审计 > 日志投递。
- 2. 如果日志投递未配置,则直接进入配置页面;如果日志投递已配置,单击**重新配置**进入配置页面。
- 3. 在配置页面,配置日志投递信息。

	投递配置			
체료 · · · · · · · · · · · · · · · · · · ·	网络接入方式:	○ 支撑环境接入 ○ 公网域名接入		
RALI Column Column RALI Column Column <thcolumn< th=""> <thcolumn< th=""> Colum</thcolumn<></thcolumn<>	消息队列实例:	请选择	φ	
Topic ID BBABE DBABE Topic Id/SBR audiog BILB BILB <td>• 网络:</td> <td>请选择</td> <td></td> <td></td>	• 网络:	请选择		
audiog 审计定意 审计定意日志 语言问 · riskog 时计规定 审计规定日志 语言问 ·	Topic ID	日志类型	日志说明	Topic Id/名称 (j)
riskog 單计與脸日志 급击师 국		audilog 审计日志	审计全量日志	请选择 ▼
		risklog 审计风险	审计风险日志	请选择
	保存生效	测试		

参数列表:

参数名称	参数说明
网络接入方式	选择消息队列的接入方式。
消息队列实例	选择日志投递的消息队列实例。
网络	选择需使用的网络,支持 PLAINTEXT 类型。
用户名	设置用户名。仅公网域名接入方式需要填写。
密码	设置密码。仅公网域名接入方式需要填写。
Topic ID/名称	选择投递的 Topic。

4. 输入参数后,单击**保存生效**。



日志管理 日志备份管理

最近更新时间:2025-05-26 18:00:22

用户日志存储空间划分为在线日志、备份日志两部分,两者比例为7:3。最新产生的日志为在线日志,可在查询分析页面查看。当在线日志存储空间占用达到 80%后,系统将把早期日志压缩存储,以节约空间,压缩比约为4:1。

() 说明:

 例如: 24 年01月23 日,用户在线日志存储空间达到80%,触发了日志备份,系统把用户在线日志中最早期的一段(如 23 年04月01日−23 年04 月30日)取出来进行压缩备份,备份后这段时间的日志会从在线空间删除,无法在审计日志页面查看,用户的在线存储空间从 80%降低到了 70%,备份后的文件可以在备份日志查看页面获取。

而在日志备份设置页面,用户设定了"备份日志保留时长"为6个月,代表该日志备份文件如果6个月内未手动恢复(操作单击恢复)则永久清理。如果用户希望查看这段时间的日志,需要在**在线存储空间足够**的前提下,从备份日志查看页面对目标文件进行恢复。恢复后的日志会被放回在线 日志存储空间,用户可以在审计日志页面重新查询到。

• 如果在线存储空间不足,可以通过存储扩容保留更久时长的日志。

备份设置

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击基础审计 > 日志管理。
- 2. 在日志管理页面,单击**日志备份设置**。
- 3. 在日志备份设置页面,设置日志备份的相关参数,单击保存。

日志新扮说置 各份日志宣者 日志祝敏 日志日	服务CLS 配置备份		
① 当在然日本法则在然日本地定空间40%利,将自动以交升形成日 日本条条成功后,用利在在然日本用制制,各会日本用有利用	3.88各份依平日志、压缩比约为4:1。 3.88者。		×
 金付日本料面料長 ● ↑月 ① ● ★ ① 			
80			

参数说明:

- 备份日志保留时长:备份日志存储超过该时长即永久删除。
- 恢复日志保留时长:备份日志只有执行恢复操作后才能查看,恢复日志最多保留7天(含恢复当日)。

备份日志查看

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击基础审计 > 日志管理。
- 2. 在日志管理页面,单击**备份日志查看。**
- 3. 在备份日志查看页面,通过日志起始时间、结束时间确认需要查看的备份日志。

日志後份设置 备份日志宣看 日志脱敏	日志服务CLS 配置备份			
· SORLUZARAINON, BRRONDANI	26.			×
2825 01-01 00:00 00 - 2025 02-28 00:00:00 [1]				
BARMNA +	日本出現的问	重极大小	日本秋志 〒	16.07

4. 日志状态为**备份文件**的日志,可以单击恢复。

2022-06-15 21:42:36	2022-06-15 22:22:54	493MB	• 已恢复	恢复 查看 删除备份
2022-06-15 21:21:48	2022-06-15 21:48:20	488MB	• 备份文件	恢复 查看 副除备份

5. 在确认恢复弹窗中,给出了预估的恢复时间,单击确定后等待恢复完成。



		×
确定恢复该日志?		
该备份日志恢复预计需要2小时		
确定	取消	

6. 恢复完成后,其日志状态变更为已恢复。单击操作列的**查看**,弹出日志查看页面。

备份日;	志查看					
2022-0	06-15 21:42:36 ~ 2022	-06-15 22:22:54 📋	高级筛选 🔻			
序号	数据资产名称	用户名	客户端IP	时间 🕈	SQL语句	操作
1	0.000	-	1010-0010-001	2022-06-15 22:22	s	详情
2	-	-		2022-06-15 22:22	s	详情
3	6000 C	root	1110.00000	2022-06-15 22:22	s	详情

7. 若要删除备份日志,单击操作列的**删除备份**,经过二次确认后即可删除。

🕛 说明

- 备份文件只有恢复后才可查看。
- 备份文件删除之后,无法恢复,请谨慎操作。



日志脱敏

最近更新时间:2025-05-26 18:00:22

日志脱敏是指对记录在日志中的敏感数据进行处理,以实现对敏感隐私数据的安全保护。

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击基础审计 > 日志管理。
- 2. 在日志管理页面,单击**日志脱敏。**
- 3. 在日志脱敏页面,选择需要脱敏的数据规则,并将开关列中的"开启/关闭"切换为"开启"。

201	影歌声点	8.5	#%
741	建晶彩铁	報報論342年E54位	
949 2	建造影响	保服前2位相后4位	
信用卡	通過影響	保留前4位和后-4位	
	22.834	保留前4位和64位	
F-98	2110W	外期前5位相信5位	
118	湖道影響	9 Million Contraction of the Con	
創稿	NERS	保留第2位和后+拉	
车就号码	22538	保留前2位程后2位	



日志服务 CLS

最近更新时间: 2025-05-26 18:00:22

数据安全审计支持将审计日志投递到日志服务 CLS,实现日志从采集、日志存储到日志检索等全方位的日志服务。

说明:
 日志服务 CLS 为第三方独立计费云产品,计费标准请参考 CLS 购买指南。

前置条件

- 已开通 数据安全审计服务。
- 已开通日志服务。
- 当前账号已完成角色授权。

开通日志服务与角色授权

首次使用时,您需要 <mark>开通日志服务</mark> 并完成角色授权。

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击基础审计 > 日志管理。
- 2. 在日志管理页面,单击**日志服务 CLS**。
- 3. 在日志服务 CLS 页面,单击**前往授权**,弹出服务授权弹窗。

```
    () 將數据安全审计的审计日志投递至CLS日志服务需完成以下开通/授权操作
    ● 已完成CLS日志服务开通 
    ● 目前暫未为CDS创建服务角色,请前任授权
```

- 4. 在服务授权弹窗中,单击**同意授权**,即可完成授权操作。
- 5. 操作完成后,即可使用日志服务 CLS,实现将审计日志、风险日志从采集、日志存储到日志检索等全方位的日志服务。

启用日志服务CLS

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击基础审计 > 日志管理。
- 2. 在日志管理页面,单击日志服务 CLS。
- 3. 在日志服务 CLS 页面,选择需要启用的日志类型,单击**立即启用**,即可弹出开启日志投递的弹窗。

审计日志投递至CLS日志服务	风险日志却进至CLS日志服务
CLS日志服务为第三方独立计数元产品,计师和道法参考CLS计数据通	CLS日志福务为第三方独立计数元产品。计数标准读号内CLS计数相述
UERREGUILERS, REGUILERSENNUERREEN, VER. ST. BENITER	UZURECHICARE, NOCHZARMANNIZZYCZY, NR. BR. BRUING

4. 在开启日志投递的弹窗中,选择目标地域、日志集、日志主题等配置。

开启日志投递	2				×	
目标地域	广州	•				
日志主题操作	◯ 选择已有日志主	题 创建日志主题				
日志集		v				
國主志日		•				
			1即开启 关键	đ		
参数	i	说明				
目标地域	;	选择日志投递的地	域,支持异地投	递。		



日志主题操作	日志主题是日志数据进行采集、存储、检索和分析的基本单元。支持选择已有日志主题或者创建日志主题。
	 选择已有日志主题:可在搜索框筛选所选日志集下的日志主题。 创建日志主题:在所选日志集下创建新的日志主题。
日志主题	 说明: 您可对日志主题进行管理,详细请参见管理日志主题。
日志集操作	日志集是对日志主题的分类,方便您管理日志主题。支持选择已有的日志集或者创建日志集。仅当日志主题操作选择创建日 志主题时可选。
日志集	 选择已有日志集:可在搜索框筛选已有的日志集。 创建日志集:仅当日志主题操作选择创建日志主题时,此项可设置。

5. 选择参数配置后,单击**立即开启**即可。

检索分析

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击基础审计 > 日志管理。
- 2. 在日志管理页面,单击**日志服务 CLS**。
- 3. 在日志服务 CLS 页面,选中需要查看的日志类型,单击检索分析,跳转至 日志服务控制台。
- 4. 在日志服务中,检索分析提供对日志数据进行过滤、搜索和统计分析的功能。
- 5. 详细请参见检索分析。

关闭投递

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击基础审计 > 日志管理。
- 2. 在日志管理页面,单击**日志服务 CLS**。
- 3. 在日志服务 CLS 页面,选择需要关闭的日志类型,单击关闭投递,弹出关闭投递的弹窗。
- 4. 在关闭访问日志弹窗中,阅读注意事项并勾选确认关闭,单击确认即可。

关闭访问日志	×
() 关闭日志投递后,将停止投递数据安全审计日志。	
确认关闭 注意:关闭日志投递后,仅停止新增日志的投递, <mark>存量日志将持续存储在日志主题中直至</mark> 期,期间将持续产生存储费用。若需删除日志主题,请前往日志主题管理删除。 	过
① 说明:	

- 关闭日志投递后,将停止投递数据安全审计日志。
- 关闭日志投递后,仅停止新增日志的投递,存量日志将持续存储在日志主题中直至过期,期间将持续产生存储费用。若需删除日志主题,请前往
 日志主题管理 删除。



风险识别 审计风险

最近更新时间:2025-05-26 18:00:22

审计风险从审计规则命中的风险等级维度,帮您进行安全分析。

检索审计风险

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**安全运营 > 风险识别**。
- 2. 在审计风险页面,可根据具体数据资产名称检索,还可以按最近一小时、今天、昨天、本周、上周、本月、上月、近半年、自定义日期检索。

200805	ν" ·	2025-02-06 14 21 57 - 2025-02-06 15 21 57 🛗 高級構造 *		
18-10	BHE/*88	<u>最近</u> 一の51 今天 昨天 本羽 上周 本月 上月 近年年	流动未過 Y	风能等量 # 00L适句 路作
1	-	ENG.A	元(3365	1700 DELETE WWW. BRUNN
2	-	B - 二 三 四 五 六 日 - 二 三 四 五 六 日 - 二 三 四 五 六	2.5.88年	428 DELETE 711 (12.103)
з	-	29 30 31 1 2 3 4 26 27 28 29 30 31 1 5 6 7 8 9 10 11 2 3 4 5 6 7	艺教授师	HAN DELETE IVM ENDEM
4	-	12 13 14 15 16 17 18 9 10 11 12 13 14 15	7.0384	40.8 DELETE OTH MARK
5	-	19 20 21 22 23 24 25 16 17 18 19 20 21 22 26 27 28 29 30 31 1 23 24 25 26 27 28 1	25997	4928 DELETE 71% dizion
6	-	italitation data	元的20%	1928 DELETE IVW SILING

3. 如需对审计风险进行指定检索。单击**高级筛选**,可根据用户名、命中规则、风险等级、客户端 IP 等关键字,输入具体值,单击**查询**,即可查看相关信息。

2003	R/* *	2025-02-00 14 20 21 ~ 20	15-02-08 15:28:21	高级算选 -					
18-19	BHE/*68	8.00	8.PMP	R261 #	命中规则	流至央源 T	风险等级 羊	SQLIER	80
1	-	-	****	2025-02-08 15:25	无share无新成 期 降	云放艇库	⇒RJ9	ROTTER AND ADDRESS OF MIGHT AND	itte esikati
2			-	2025-02-08 15:25	Tastere进致组织的	元数据用	*RJ0	\$111.118 (mode, 1686) (million of 1686) (million)	I'M BERNEN
э			-	2025-02-08 15:24	无where決測成觀測	乙酸氟库		\$111.118	#41 19233
4			****	2025-02-08 15:24	Xature 2.814.803	云数最库		\$111.108 (and), folia: an integr ? and	ITTO ESHENCIU

查看数据详情

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击安全运营 > 风险识别。
- 2. 在审计风险页面的日志列表中,选择所需日志,单击**详情**,进入审计风险详情页面。

25035	0 ⁴ •	1025-02-00 14 20 21 - 2025	-42-08 15 28 21	高級路送 ~					
18-16	数据资产648	MP6	医疗論弁	RH #	命中規則	这是来源 Y	风险等级 羊	SQL 1819	515
1	-		****	2025-02-08 15:25	表where 把新生的数	元数制作	中风险	DELETE	716 BB
2			-	2025-02-08 15:25	无where更数或删除	乙酸碱库	中风险	DELETE	911 ER
з			-	2025-02-08 15:24	无where更新或删除	元数据库	17.82	DELETE	215 E.E.E
4			-	2025-02-08 15:24	无where把IS图刷	四股銀座	49.8.82	DELETE	91 BR



3. 在审计风险详情页面,可查看该条日志的基本信息和详细信息。

审计风险详情		×
基本信息		
操作语句	DELETE FROM 展开	
操作类型	DELETE	
事件类型	DML	
操作时间		
SessionId	CONTRACTOR OF CONTRACTOR	
命中规则	无where更新或删除	
风险等级	中风险	
数据库类型	MYSQL	
数据库IP	10.00.000	
数据库用户		
客户端IP	Marcan 2011	
客户端MAC		
客户端主机名	100101100	
详细信息		
数据库	-	
表名		
字段名	-	
影响行数	1	
执行时间	202 ms	
返回消息	-	
返回码	0	
包长度	67	
使用工具	-	

创建规则

您可以针对某一条风险的具体操作动作,单独创建一条审计风险规则。通过这一规则,精准锁定特定的客户端、服务端以及操作行为,实现针对性的风险管控。 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**安全运营 > 风险识别**。

2. 在审计风险页面的日志列表中,选择所需日志,单击**创建规则**,进入创建规则页面。

20810	n -	2025-01-01 00:00:00 - 202	-01-31 23:59:59 🛅	8983 -					
89	BERASA	876	808P	15H z	\$-18H	XERE Y	RINGE :	50L840	80
1		-	****	2025-01-31 23:59	2x4cer#201800	1523	98.0	DELETE FROM	1712 6512,5231
2		-	****	2025-01-31 23:59	2xtore#2id200	1525	93.80	DELETE FROM	111 012308
		-	****	2025-01-31 22:58	2xtore#2id200	17.53.2.F	PALIE	DOLETE FROM	111 (10.000
•		-	****	2025-01-31 22:58	Subort #214388	17.55 M.F	POLIE	DOLETE FROM	111 (101.008

3. 在创建规则页面,您可以看到触发数据安全风险的客户端信息、服务端信息、具体操作行为。您可以自定义规则类型、规则名称、规则备注、风险等级以及是 否告警,单击**确定**保存。



Image: Image	创建规则						>
● 思名中 ○ 自名中 ● 思名中 ○ 自名中 ● 思名中 ○ 自名中 ● 思名中 ○ 中凡世 ○ 百八日 ● 和田 ○ 市山 ○ 百八日 ● 和田 ○ 日 ● 日 ● 日 ● 日 ● 日 ● 日 ● 日 ● 日	基础信息						
北限名称: 天whore更新或服除_ 規則名称: 操作規則 • 风悠容 (● 中风) ● 中风 ● 高风) 客户语 名 ● 中风 ● 高风 客户语 名 ● 中风 ● 高风 服成年 包 ● 中风 ● 百八 ● 「日〇 ● ● 四 服成年 包 ● ● 「日〇 ● ● 四 服成年 包 ● ● 「日〇 ● ● ○ ● ○ ● ○ ● ○ ● ○ ● ○ ● ○ ● ○ ● ○	规则类型:	◯ 黒名单	白名单				
展報註: 単位 数 ● 現 数 ● 中 段 ● 中 段 ● 再 段 ● 再 段 ● 再 段 ● 再 段 ● 再 段 ● 市 座 ● 目 ● 日 ● 日 ● 日 ● 日 ● 日 ● 日 ● 日 ● 日 ● 日	▶ 规则名称:	无where更新或	11除_				
代	规则备注:	操作规则					
Rytr X SP ''Bip: E S < Is Is SP ''Bip: E S <	风险等级:	🗌 低风险 🔵	中风险 高	高风险			
客户端 客户端 自合 16/ 解 服务端 取取用 自合 172 解 取取用 第子 - 3306 + 解 取取用 172 第 - 3306 + 解 取取用 172 - 3306 + 解 取取用 日合 - 3306 + 解 取取用 日合 - - 3306 + 解 日数 日 - - 3306 + 解 日数 日合 - - - - - 日 日 日 -	规则定义						
服务程 数取用p: 包含 72 解除 数取序箱口: 等于 - 3306 + 新除 数取序用P: 包含 一 3306 + 新除 数取序名: 包含 可尼置多个数取序名,英文逗号分隔,如: mysql,tost 新除 時 日合 可尼正TE FROM ' 新除 表名: 包含 ● ●	客户端:	客户端ip:	包含	Ŧ	16:	删除	
数据库福口: 答子 - 3306 + 解除 数据库用户: 包含 可配置多个数据库名,英文说号分幅,如: mysql,tost 解除 数据库名: 包含 可配置多个数据库名,英文说号分幅,如: mysql,tost 解除 行为: 操作奖号: 包含 DELETE 解除 操作语句: 包含 DELETE FROM '	服务端:	数据库lp:	包含	Ŧ	172.	删除	
数据库用户: 包含 可配置多个数据库名,英文混号分隔,知:mysql,tost 邮除 方方: 操作进行: 包含 可配置多个数据库名,英文混号分隔,知:mysql,tost 邮除 操作进行: 包含 DELETE 邮除 表名: 包含 DELETE FROM ' 邮除		数据库端口:	等于	Ŧ	- 3306 +		
数据库名: 台合 可配置多个数据库名,英文进号分隔,知:mysql,test 課館 行为: 操作英型: 台合 DELETE 課館 操作语句: 台合 DELETE FROM '		数据库用户:	包含	Ŧ		删除	
行为: 操作类型: 包含 ▼ DELETE ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		数据库名:	包含	Ŧ	可配置多个数据库名,英文逗号分隔,如:mysql,test	副餘	
操作语句: 包含 ▼ DELETE FROM ' 翻除 表名: 包含 ▼ hoor	行为:	操作类型:	包含	Ŧ	DELETE	副除	
表名: 包含 v hoor ####		操作语句:	包含	Ŧ	DELETE FROM `	删除	
â出走义		表名:	包含	Ŧ	hear	副除	
俞出定义							
	會出定义						
	确定	取消					



模型风险

最近更新时间:2025-05-26 18:00:22

模型风险基于智能风险模型监测结果进行统计,可以查看详细的风险信息,并支持对风险事件的状态进行更改。

检索模型风险

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击安全运营 > 风险识别。
- 2. 在审计风险页面,单击模型风险,进入模型风险页面。
- 3. 在模型风险页面,可以按最近一小时、今天、昨天、本周、上周、本月、上月、近半年、自定义日期进行风险检索。

我最后规	20	024-0	X6-04	15:36	14	- 202	-02-0	8 15:3	6.14 (1								_						多个过速局望用同年级分数	Q Q
BER/ 8	ļ	-	iii-	040		9 天		帅天	*	19	±٨		*月		±Л		649			氨型分类 T	风险等量 T	W語 T	8.9		
	L	n	定义																	异常行为模型	ARM	#X12	i 1 10 - 51	en e	
	2	20243	₩ aF	9				4	• •		2005	# 2月					•	•		数据波察模型	高风险	新发现	1998 - 19	en e	
	١.	8 28	28			Ξ 31	1	五 2	六 3		8 26	27		. <u>=</u> 5 21	1 8 0 1	9 3 0 3	Б. : П	六 1	1	异营行为模型	有风险	B 83	17M - 8	ent.	
-	١.	4	5	6		7	8	9	10		2	3	4	5		3	7	8		异常行为模型	ARM	#2.12	itm 15	-	
-	ł.	11	12	2	3 0	14 21	15 22	16 23	1/ 24		9 16	10	11	12	; 1) 2	0 :	4 11 :	15 22	3	异营行为模型	消风险	新发现	174A - 52	an a	
	Ŀ	25	20	5 2	7	28	29	30	31		23	24	25	5 20	5 2	7 3	18		,	教授地部模型	高风险	#X1	17M - 12	a	
	1	8114	94														R Z			计算机 实现	ARM	82.0	inn - 11	a contraction of the second	

() 说明:

因模型风险需要基于最近7天的时间动态建立基线,所以风险详情识别周期 ≥ 模型开启后7天。

查看模型风险详情

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击安全运营 > 风险识别。
- 2. 在审计风险页面,单击模型风险,进入模型风险页面。
- 3. 在模型风险页面的列表中,选择需要查看的风险,单击**详情**。

2824-08-88 15:36:14 - 2825-62-88 15:36:1						STERRENTWON Q
数据数件名称	108	模型名称	模型分类 T	风险等级 Y	联西 T	油 作
	2025-02-05 15:54:31	从新的末期中世界教育家	异常行为模型	再见数	8X1	17M 52/2
	2025-01-20 09:40:00	数据查询至符合	計算改造模型	A .R.M	新发现	1715A S52W
	2025-01-09 11:0218	从新的未超中世界致影响	异常行为模型	泉泉融	#X11	1714 SER
	2025-01-06 20:57:03	从新的来源中世界数据库	异常行为模型	消失能	新发现	1715A S528E
	2024-12-23 18:01:48	从新的来源中世界致影响	异常行为模型	8.8M	22 1	1719 SLIZ

4. 在风险详情页面,可查看该条风险的基本信息、风险信息以及处理记录。

风险详情	×
基本信息 数据资产名称	
风险发现时间	2025-04-17 16:49:43
操作行为时间	2025-04-17 16:49:38
模型名称	从新的来源IP查询数据
风险等级	高风脸
风险信息	
异常偏差	于2025-04-17 16:49:38使用新的来源IP 🔳 🔳 🔳 查询数据
模型基线	后台根据历史来源IP建立安全基线:
	当来源IP不在基线范围时,触发安全风险
处置建议	排查是否为业务变更或员工正常操作。如果以上都不是,请及时联系安全专家对告警进行调查取证和处 <mark>计。点击查看详细</mark> 操作日志
处理记录	
事件核查结果	新发现
备注	-



5. 单击点击查看详细操作日志,可跳转到对应的审计日志或者审计会话页面。

计日志	审计会话								
	• •	2025-04-17 16:49:38	~ 2025-04-17 16:49:38 📋	高级筛选 ▼					4
序号	数据资产名称	用户名	客户端IP	时间 \$	命中规则	流量来源 ℃	风险等级 ‡	SQL语句	操作
1	c	d# 🔳 💷 I	No	2025-04-17 16:49	信任select	云数据库	高风险	•	详情
共1条							10 ~ 条 / 页	н 4 1	/1页 ▶ ▶

风险核查

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击安全运营 > 风险识别。
- 2. 在审计风险页面,单击**模型风险**,进入模型风险页面。
- 3. 在模型风险页面的列表中,选择需要查看的风险,单击**处理**。
- 4. 在处理窗口中,依据具体的风险详情进行风险事件核查状态标记,单击确定。

处理		×
* 事件核查结果	@确认风险并已处理 @确认误报 @ 加白名单	
备注	请输入	
	确定 取消	



审计报表

最近更新时间: 2025-05-26 18:00:22

数据安全审计报表提供了多种报表模板,以满足不同的分析需求。这些报表包括综合分析报表、等保参考报表、性能分析报表、语句分析报表、会话分析报表。

新建报表任务

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击安全运营 > 审计报表。
- 2. 在报表列表页面,单击**报表任务**,进入报表任务页面。
- 3. 在报表任务页面,单击**新建任务**。

审计报表												回快速指引
报表列表	报表任务											
新建任务	803									请输入任务名称	現象	Q Ø
任务名	称	报表类型 ▼	报表说明	报表模版 ▼	包含资产	创建省	下次启动时间 \$	报表状态 ① 🕈	已生成报表数	任务启停	操作	
	A7.0	门 周期报表		综合分析报告	全部资产	constangest-	1000 AN 10 11 10 100	③ 待生成	1		9848 .008	

- 4. 在新建任务弹窗中,可选择单次报表或周期报表,并配置相关参数。
- 单次报表:数据安全审计管理系统支持即时生成报表,即生成某个时间段内的报表。

新建任务	×	
• 报表类型:	 ○ 单次报表 ○ 周期报表 □ 即时生成报表 ○ 建立周期性报表任务,届时自动生成报表 	
• 任务名称:	输入报表名称,最多64字符	
	报表名称将复用此任务名称	
报表说明:	输入报表说明,最多256字符	
	0 / 256	
• 报表模板:	综合分析报告	
• 包含资产:	全部资产 ▼	
• 时间范围: 힋	近24小时 🔻	
报表通知:	报表生成后将自动发送到所配置的通知范围	
	确定取消	

参数说明:

- 任务名称: 自定义名称,在64个字符之内,不能重复。
- 报表说明:自定义描述,在256个字符之内。
- 报表模板:当前审计报表支持选择综合分析报表、等保参考报表、性能分析报表、语句分析报表、会话分析报表。
- 包含资产:根据实际需求选择资产。
- 时间范围:根据实际需求选择时间。
- 周期报表:当重复周期选择定时时,数据安全审计管理系统则定时生成报表。

🔗 腾讯云

新建仕务		×
▪ 报表类型:	● 単次报表 即时生成报表 ● 周期报表 建立周期性报:	表任务,届时自动生成报表
* 任务名称:	输入报表名称,最多64字符	
	报表名称将复用此任务名称	
报表说明:	输入报表说明,最多256字符	
		0 / 256
• 报表模板:	综合分析报告	v
- 句公次在,		
• UBM/:	全部资产	~
* 时间范围:	近24小时	-
• 重复周期:	请选择 🔻	选择时间
任务启停:		
报表通知:	报表生成后将自动发送到所配置	们的通知范围
	确定取消	
会 <u>新</u> 兴田 •		

参数说明:

- 任务名称: 自定义名称,在64个字符之内,不能重复。
- 报表说明:自定义描述,在256个字符之内。
- 报表模板:当前审计报表支持选择综合分析报表、等保参考报表、性能分析报表、语句分析报表、会话分析报表。
- 包含资产:根据实际需求选择资产。
- 时间范围:根据实际需求选择时间。
- 重复周期:选择生成报表的周期
- 任务启停:设置任务启动或停止。

查看报表

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**安全运营 > 审计报表**。
- 2. 在审计列表页面,可查看内容包括报告名称、报表类型等字段。可按照报告名称对报告进行搜索。
- 3. 单击操作列的预览,可查看对应的报表。
- 4. 单击操作列的下载,可下载对应的报表至本地查看。



审计规则

最近更新时间: 2025-05-26 18:00:22

数据安全审计提供审计规则管理功能,您可以直接开启系统内置审计规则,也可自定义审计规则,以实现特性化场景需求。

规则说明

数据安全审计提供三种类型的规则:

类型	应用场景	说明
风险监测(黑名单)	用于检测数据库操作中的异常行为,当出现不符合正常操作模式的行为时触发告 警。	使用风险识别规则检测异常操作。审计 记录命中配置并启用的风险识别规则 时,会触发告警。
信任规则(白名单)	适用于对已知安全、可信任的数据库操作进行定义,以便在审计过程中对这些操 作进行特殊处理。 例如:互联网金融行业:对于已备案且合规的第三方支付机构按正常流程进行的 资金结算、清算等数据库操作,设定信任规则,确保业务顺畅同时精准审计异 常。	使用信任规则可定义您信任的操作。如 果您需要审计某类数据库操作,但无需 上报告警,您可以为此类数据库操作自 定义信任规则,帮助您提高告警准确 率。
过滤规则	主要用于筛选出不需要审计的操作,减少无效审计信息,优化审计日志管理。	使用过滤规则可定义您信任的操作。系 统不审计您在过滤规则中定义的操作, 帮助您提高告警准确率,并节省审计日 志存储空间。

审计规则触发匹配的流程如下,通过以下流程处理最终判断和产生审计日志或风险:



规则启用

在规则启用页面,您可以针对数据资产维度,进行规则的启用和禁用。

快捷配置

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**安全运营 > 审计规则**。
- 2. 在规则列表页面,单击规则启用,进入规则启用页面。
- 3. 在规则启用页面,单击快捷配置,弹出快捷配置弹窗。

审计规则					ビ 操作指南
规则列表规则启用					
-					请能入规则省称撤来 Q Ø
规则名称	规则分类 T	规则属性 T	规则类型 ▼	风险够吸 T	规则开关 T
	违规操作	内置规则	無名単	海风脸	
	注入攻击	内置规则	黑名单	海风险	



 在快捷配置弹窗,选择需要快捷配置规则的资产(也可选择所有资产),并选择适合的快捷配置组,单击确定即可完成配置,配置后将覆盖当前该资产的规则 启用配置。

① 说明
• 资产开启审计权限时,已默认开启常见配置规则。
• 规则列表中,规则名称后已添加其所属的常见配置标识。

快捷配置确认		×
数据资产	Ŧ	
启用常见风险规则,适用于大多数场景。		
确定 取消		

启用规则

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**安全运营 > 审计规则**。
- 2. 在规则列表页面,单击规则启用,进入规则启用页面。
- 3. 在规则启用页面,支持启用单个规则或批量启用规则。
 - 单个:选择所需规则,单击规则开关列的◯____,弹出"确认开启"弹窗。

规则列表 规则启用					
• 89	0.0 Sime				
11.11名称	規則公共 Y	規則属性 Y	無形失型 Y	风险等级 Y	规则疗关 T
	注入政由	內面規則	展名单	ФЯМ	
	注入段击	內面規則	黑名单	498M	
■ MyOQL-系统表面向操作	法规解作	02300	黑名单	(IXN)	
	造成操作	02300	里名单	11.7.N	
	达双脉作	ARXMM	黑名单	11.R.M	

- 批量:选择一个或多个规则,单击左上角的**启用**,弹出"确认开启"弹窗。
- 4. 在 "确认开启" 弹窗中,单击确定,即可启用对应规则。

停用规则

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**安全运营 > 审计规则**。
- 2. 在规则列表页面,单击**规则启用**,进入规则启用页面。
- 3. 在规则启用页面,支持停用单个规则或批量停用规则。
 - 单个:选择所需规则,单击规则开关列的____,弹出"确认关闭"弹窗。

32,015552X 92,00 as/40						
• 84	9/0 9 282				10	NARRENTER Q O
10564	開始分長 Y	規則属性 Y	無形失型 Y	风险等级 Y	规则开关 T	
	法入政法	內面規則	展名单	498M		
	注入 現書	內面規則	黑名单	498M		
MyOQL-系统表面和操作	3.8847	自定实现则	黑名单	62N		
	1.52117	02588	里名单	62N		
-	造双脚作	REXMN	2 8.0	11.7.1k		

- 批量:选择一个或多个规则,单击左上角的**停用**,弹出"确认关闭"弹窗。
- 4. 在"确认关闭"弹窗中,单击确定,即可停用对应规则。

规则管理



查看规则

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**安全运营 > 审计规则**。
- 2. 在规则列表页面,可查看系统提供的内置规则和自定义规则。

新建规则

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**安全运营 > 审计规则**。
- 2. 在规则列表页面,单击**新建**,进入新建规则页面,依次配置基础信息、规则定义和输出定义。
- 基础信息

基础信息	
规则类型:	▶ 风险检测(黑名单)①
★ 规则名称:	请输入规则名称
规则备注:	请输入规则备注
★ 风险等级:	● 低风险 ○ 中风险 ○ 高风险

	参数	参数说明		
	风险监测(黑名单)	使用风险识别规则检测异常操作。审计记录命中配置并启用的风险识别规则时,会触发告 警。		
规则类型	信任规则(白名单)	使用信任规则可定义您信任的操作。如果您需要审计某类数据库操作,但无需上报告警, 您可以为此类数据库操作自定义信任规则,帮助您提高告警准确率。		
	过滤规则	使用过滤规则可定义您信任的操作。系统不审计您在过滤规则中定义的操作,帮助您提高 告警准确率,并节省审计日志存储空间。		
丸	观则名称	自定义规则名称,用于标识具体规则,长度为1–64个字符,不可重复。		
夫	观则备注	规则描述信息。		
۵	1.险等级	规则对应的风险等级,若命中规则,可在 <mark>审计风险页面</mark> 查看相关低、中、高风险日志信 息。		
计语士士	只审计风险行为(命中风险 检测规则)	仅对符合风险检测规则的操作进行审计记录,其他操作不记录,聚焦风险行为审计,减少 非风险操作日志冗余。		
₹₹₩ġŶĴĬţ	自定义过滤规则	根据自行设定的条件过滤操作,可灵活指定哪些操作不被审计,进一步精准控制审计范 围,节省审计资源 。		

() 说明:

若一个资产同时关联"只审计风险行为"过滤规则和自定义过滤规则,仅前者生效。

• 规则定义: 以下三个规则仅作为示例,且规则类型为黑名单,用户可根据自身业务自行配置。



○ 防爬取规则:防止使用例如 select 操作语句,爬取表数据。

规则定义								
客户端:	客户端IP:	包含	Ŧ	可聞	記置多个IP和网段,英文逗号分隔,如:192.168.1	.1,192	.168	添加
	客户端端口:	大于等于	Ŧ	_	0		+	添加
	客户端主机名:	包含	Ŧ	可聞	R置多个,英文逗号分隔,如:diver,Client			添加
	使用工具:	包含	v	可聞	2置多个,英文逗号分隔,如:diver,client			添加
服务端:	数据库IP:	包含	Ŧ	可言	记置多个IP和网段,英文逗号分隔,如:192.168.1.	.1,192.	.168	添加
	数据库端口:	大于等于	Ŧ	_	0		+	添加
	数据库用户:	包含	~	可言	2置多个,英文逗号分隔,如:sys,root,system			添加
	数据库名:	包含	•	可冒	2置多个,英文逗号分隔,如:mysql,test			添加
	表名:	包含	•	请辅	俞入表名,多个用英文逗号分隔			添加
行为:	操作类型:	包含	Ŧ	sele	ect			添加
	操作语句:	包含	•	请辅	â入操作语句,多个用英文逗号分隔			添加
语句执行:	执行时长:	大于等于	•	-	0	+	毫秒	添加
	影响行数:	大于等于	•	-	100	+	行	添加
	操作时间:	大于等于		请说	经日期		ö	添加
其他:	返回码:	大于等于	Ŧ	-	0	+	行	添加

○ 慢查询发现规则:检查执行时间较长的 SQL 语句,便于进行优化。



规则定义								
客户端:	客户端IP:	包含	Ŧ	可配置多个IP和网段,多	英文逗号分隔,如:192.	168.1.1,192.1	168	添加
	客户端端口:	大于等于	Ŧ	-	0		+	添加
	客户端主机名:	包含	Ŧ	可配置多个,英文逗号:	分隔, 如: diver,client			添加
	使用工具:	包含	¥	可配置多个,英文逗号;	分隔, 如: diver,client			添加
服务端:	数据库IP:	包含	*	可配置多个IP和网段,引	英文逗号分隔,如:192.	168.1.1,192.1	168	添加
	数据库端口:	大于等于	Ŧ	-	0		+	添加
	数据库用户:	包含	*	可配置多个,英文逗号	分隔,如:sys,root,syst	em		添加
	数据库名:	包含	Ŧ	可配置多个,英文逗号	分隔,如: mysql,test			添加
	表名:	包含	Ŧ	请输入表名,多个用英	文逗号分隔			添加
行为:	操作类型:	包含	Ŧ	select				添加
	操作语句:	包含	v	请输入操作语句,多个月	用英文逗号分隔			添加
语句执行:	执行时长:	大于等于	Ŧ	-	500	+	毫秒	添加
	影响行数:	大于等于	~	-	0	+	行	添加
	操作时间:	大于等于	Ψ.	请选择日期			ö	添加
其他:	返回码:	大于等于	Ŧ	-	0	+	行	添加

 \odot 危险操作规则:检查执行 delete、drop、alter 等类型的高危 SQL 语句。

🗎 添加

十行 添加

分 腾词	刑云									
10.001	÷.\.									
规则》	定义									
客户	'端:	客户端IP:	包含 🔻	可配置多	个IP和网段,英文	文逗号分隔,如]: 192.168.1.1	1,192.	168	添加
		客户端端口:	大于等于	-		0			+	添加
		客户端主机名:	包含 🔻	可配置多	个,英文逗号分	嗝, 如: diver,	client			添加
		使用工具:	包含 🔻	可配置多	个,英文逗号分	嗝, 如: diver,	client			添加
服务	3端:	数据库IP:	包含 🔻	可配置多	个IP和网段,英文	 辽逗号分隔,如]: 192.168.1.1	1,192.1	168	添加
		数据库端口:	大于等于 🔻	-		0			+	添加
		数据库用户:	包含 🔻	可配置多	个,英文逗号分降	高, 如: sys,ro	ot,system			添加
		数据库名:	包含 🔻	可配置多	个,英文逗号分降	高, 如: mysql	l,test			添加
		表名:	包含 🔻	请输入表	名,多个用英文ì	逗号分隔				添加
行为):	操作类型:	包含 🔻	drop						添加
	L	操作语句:	包含 🔻	请输入操	作语句,多个用望	英文逗号分隔				添加
语句]执行:	执行时长:	大于等于 🔻	_		0		+	毫秒	添加
		影响行数:	大于等于 ▼	_		0		+	行	添加

▼ 请选择日期

-

0

•	输出定义、	规则启用

其他:

操作时间:

返回码:

大于等于

大于等于



創出定义					
是否告警	●是○否				
则启用					
关联数据资产:	选择数据资产 (13)			已选择的数据资产 (0,	/13)
	请输入资产名称搜索		Q	数据资产名称	数据资产类型
	数据资产名称	数据资产类型			
		MySQL	î		
		MySQL			
	1011070	MySQL	•	•	
		MySQL			
		MariaDB			
		MySQL			
			-		

参数说明:

- 是否告警:根据实际需求选择是否告警。
- 关联数据资产:根据实际需求选择资产。(可选)

3. 配置完成后,单击确定即可。

修改规则

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**安全运营 > 审计规则**。
- 2. 在规则列表页面,找到需要修改的规则,单击编辑,进入编辑规则页面。

# #2# #8000 60000 1 - #80 5 #2.6 #65.000 60000 1 - #66.899 5 #2.6 #65.000 60000 1 - #66.899	規则名称	規则类型 T	规则属性 T	风险等级 下	关联数据资产	备注	操作
第二 第五条 自会以現 COUC 1 - 4編 巻き 2 第二条集 由空以現 1000000000000000000000000000000000000		黑谷单	自定义规则	低风险	1		编辑 删除
★ 単点単 自定火売時 (1) ・ 売貸 単分	□ ≍	黑名单	自定义规则	低间度	1		编辑 二 删除
		黑盔单	自定义规则	低风险	t		编辑 删除

3. 在编辑规则页面,修改信息后,单击确定即可。

删除规则

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**安全运营 > 审计规则**。
- 2. 在规则列表页面,找到需要删除的规则,单击**删除**,弹出确认删除弹窗。

第二 第五章 百五 次和 6000 1 6000 1 6000 1 6000 6000 1 6000 6000 1 6000 6000 1 6000 6000 1 6000 6000 1 6000 6000 1 1 <th1< th=""> <th1< th=""> <th1< th=""> <</th1<></th1<></th1<>	規则名称	规则类型 T	规则属性 〒	风险等级 T	关联数据资产	备注	操作
x #A# EEXXXII COUR 1 - GR BH x #A EEXXXII COUR 1 - GR BH		黑名单	自宠义规则	低风险	1	-	编辑 删除
第 単点単 自定以規則 日間 1 ・ 病機 割除	×	黑名单	自定义规则	低风险	1		编辑 一删除
	3	黑名单	自定义规则	低风险	1		编辑 删除

3. 在确认删除弹窗中,单击确定即可。


智能分析

最近更新时间:2025-05-26 18:00:22

行为模型

行为模型通过对用户行为的分析,识别出用户的正常操作模式和行为特征,帮助识别潜在的安全威胁和异常行为。系统内置丰富的行为模型,以满足大多数数据安 全场景。

关联 / 取消关联资产

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击安全运营 > 智能分析,进入行为模型页面。
- 2. 在行为模型页面,选择需要关联资产的行为模型,单击 🖍 。

行为根型 模型吊用					
				多个关键字用数括"	98. #12#9588#898 Q Ø
模型名称	模型分类 T	·杨型银行 Y	网络秘密 T	关款(25)(83)/2	88
And the second	10.000	内量	10,738	1 × 1	1990) — 4898
	10.000	内量	36740	1.2	(759) - 9678
1000000000	10.000	7. 1	10700	1.2	1759 SMAR
delenge racing with	2001-000	内藏	82709	1.2	1918 - 1904

3. 在关联资产页,选择需要关联 / 取消关联的数据资产,单击确定即可。

风险等级编辑

1. 在行为模型页面,选择需要查看的行为模型,单击操作栏中的编辑。

行为模型 模型扇用					
				多个关键字用量线 17 分	◎ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
模型名称	模型分类 〒	模型层性 Y	风险等质 Y	关联教育地产	授作
And the second sec	10,000	内置	海风险	2 /	(#55 (443)
100.01	101000	内置	海风的	12	1739 MA
100000000	101000	内置	76740	1.2	1759 - 564B
British Includes	101108	内置	20135	1.2	洋橋 编辑

2. 在编辑模型页面,修改等级后,单击确定即可。

查看详情

在行为模型页面,选择需要查看的行为模型,单击操作栏中的**详情** ,即可进入详情页,查看该模型的具体风险信息。

模型启用

在模型启用页面,可以在数据资产维度,进行模型的启用和停用。

启用模型

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**安全运营 > 智能分析**,进入行为模型页面。
- 2. 在行为模型页面,单击模型启用页签,进入模型启用页面。
- 3. 在模型启用页面,支持启用单个模型或批量启用模型;
 - 单个:选择所需模型,单击模型开关列的◯___,即可启用对应模型。

2018分析 ③ 東通三 ~ 行力構築 機能取用				
• 508 508				Strutter ton. Structure Q
機型名称	模型分类 T	模型规注 Y	542010EL Y	65202/8
10101070	10.045	内置	16503	
1001001	101000	内量	36738	
and the second s	101000	内重	10708	
energi su travel	101100	内量	26746	

○ 批量:选择一个或多个模型,单击左上角的启用,即可启用对应模型。

停用模型

在模型启用页面,支持停用单个模型或批量停用模型。

• 单个:选择所需模型,单击模型开关列的____,即可停用对应模型。



MBCODI (O HOL -				
行为编型 模型応用				
908 903				STARTER TOR. STOREERS OF Q
- ##25/0	模型分类 平	模型原性 Y	网络琴技 Y	R2258
1001001	10.000	内量	14R49	
and the second sec	101000	内量	16749	
ALCONO DE LA CONTRACTA	101000	内量	16740	
Britra Inches	001100	内量	11R30	

• 批量:选择一个或多个模型,单击左上角的停用,即可停用对应模型。

智能分析风险查看

智能分析模型开启后,需要有7天的时间动态建立基线,当基线建立后,即可通过 模型风险 查看具体风险内容。





最近更新时间: 2025-05-26 18:00:23

用户可以在告警历史页面查看近期收到的告警记录。

说明:
 支持查看近30天内的告警。

查看告警历史

1. 登录 数据安全审计控制台,在左侧导航栏中,单击系统管理 > 告警管理。

2. 在告警历史页面,可以查看近期收到的告警。支持自定义时间段,以及根据告警类型、告警级别、告警 ID 进行筛选和匹配。

- 告警 ID: 告警记录的唯一ID。
- 告警时间: 该条告警产生的时间。
- 告警类型:包含审计风险、模型风险、自审计风险、Agent 掉线、QPS 超限、存储超限,支持筛选。
- 告警级别:包含高风险、中风险、低风险,支持筛选。
- 聚合次数:表示该告警包含的风险数。若为实时风险触发的告警,聚合次数为 1;若为聚合后发出的告警,则记录了时段内包含的风险个数。

2025-04-18 00:00:00 ~ 2025-04-18 10:58:20					多个过滤标签用回车输分隔	Q <i>Q</i>
告答iD	告誓时间	告酬类型 🔽	告警级则 ▽	聚合次数		操作
alar	2025-04-18 10:07:42	审计风险	高风险	1		s¥tm
ələr)	2025-04-18 10:07:41	审计风险	高风险	1		3¥1 8
alar	2025-04-18 10:07:40	审计风险	高风险	1		setm
ələr	2025-04-18 10:07:39	审计风险	高风险	1		详细
ələr	2025-04-18 10:07:38	审计风险	高风险	1		详细
ələr	2025-04-18 10:07:37	审计风险	高风险	1		seta
ələr	2025-04-18 09:00:10	审计风险	高风险	1000		洋橋
ələr	2025-04-18 09:00:10	审计风险	任风险	1000		seta
ələr	2025-04-18 09:00:10	审计风险	中风险	80		3¥1 6
ələr	2025-04-18 08:25:35	自审计风险	任风险	1		详细
其 33 条				10 ~ #	/页 ∺ ◄ 1 /4	д н н

查看风险详情

- 1. 在告警历史页面,选择目标告警,单击操作列的详情。
- 2. 在告警详情页,单击**基本信息**,查看告警的基本信息,包括告警时间、告警类型、告警级别、风险数量。

← alarm-	· · · · · · · · · · · · · · · · · · ·
基本信息	风险信息
告警时间	2025-04-18 09:00:10
告警类型	审计风险
告警级别	中风险
风险数量	80

3. 在告警详情页,单击**风险信息**,在风险信息页面,详细的记录了该告警中的风险详情。包含审计风险和模型风险。您可以在风险信息内直接对相应风险进行查 看和处置。

○ 审计风险告警关联的风险信息示例:



← alarm-											
基本信息	风险信息										
③ 当页风险数据	○ 当然风险数据可能不多于我台风越想:历史日志金付短期的机,历史和脉不定并但主能开展展示,可能注 <u>者过日意</u> 物意识的计词段日志与用金者。										
全部数据资产	~	2025-04-18 07:00:05 ~ 20	125-04-18 09:00:05	高级转送 ▼							
序号	数据资产名称	用户名	客户端IP	8349 \$	命中规则	法量未添 豆	风险等级 1	SQL语句	操作		
1	cc	root		2025-04-18 08:00	MySQL-系统表查询操作2	Agent	中风险	•	init clange		
2	60	root		2025-04-18 08:00	MySQL-系统表面询操作2	Agent	中风险		SPHW SERVICEJ		
3	66	root		2025-04-18 08:00	MySQL-系统表查询操作2	Agent	中风险	s :	init status		
4	cc	root		2025-04-18 08:00	MySQL-系统表面询操作2	Agent	中风险		VIEW SERVICE		
5	00	root		2025-04-18 08:00	MySQL-系统表面询操作2	Agent	中风险	•	洋情 创建规则		
6	cc	root	2	2025-04-18 08:00	MySQL-系统表查询操作2	Agent	中风险		STAN ELEMENT		
7	00	root		2025-04-18 08:00	MySQL-系统表面询操作2	Agent	中风险		洋情 创建规则		
8	cc	root		2025-04-18 08:00	MySQL-系统表查询操作2	Agent	中风险		THE REPORT		
9	00	root	10.00	2025-04-18 08:00	MySQL-系统表查询操作2	Agent	中风险	•	詳情 创建规则		
10	cc	root	1000	2025-04-18 08:00	MySQL-系统表查询操作2	Agent	中风险	4	i#f# tilikkenj		
共 80 条								1~条/页 日	і 4 1 /8页 ► н		

·	- alarmana and and and and and and and and and						
	 当页风险数量可能不等于聚合风险数:历史日; 	志备份成删除时,历史风险不支持在当前页襄展示,可前行	E <u>备份日志</u> 恢复该时间段日志后再查看。				
	문문화 2025-04-17 15:49:44 -	~ 2025-04-17 17:49:44 🗄					多个过滤标签用回车键分隔 Q 2
	数据资产名称	操作行为开始/结束时间 风险发现时间	模型名称	模型分类 ▽	风险等级 订	秋章 卫	操作
		2025-04-17 16:49:38 2025-04-17 16:49:38 2025-04-17 16:49:43	从新的来源印查询数据	数据泄露	赛风险	新发现	详情 处理
○ 模型风险告警关联的风险信息示例:	共1条						10 ∨ ∯/д н ч 1 /1д ⊨ н

告警跳转

()

用户可以通过收到的告警内的链接直接跳转到对应页面。

说明:		
支持站内信、邮件内容的告警跳转。		

1. 在站内信页面,用户可以查看风险触发的告警信息。

消息中心	← 数据安全审计告警	2025-04-18 10:07:42		L-M T-M
 ↓ 站内信 ↓ 订阅管理 				
2 接收管理 、			【数据安全审计】告警	
			碁歌的機讯云用户、您好! 您的横讯五张号(张号D:1 4, 把称: 数) 前段页的 数据安全审计产品,于1040741, 触发审计规则高风险告誓 1次, 告誉地址:普通区,告 警UD为: / 3,点击"亚者详情"进入产品控制台查者。	
			查看详情	
			此效 時讯云团队	
			久は高格子,林安理室立東面 Copying 2013 - 2025 - 2025 - 2025 Al Rights Reserved. 時改五 配灯所有	

2. 单击**查看详情**,可以跳转到告警相关页面,并通过告警 ID 自动定位到对应告警。可以参考上文进行告警详情的查看和处置。

告警历史 告警设置					
 支持查看近30天告警。默认展示当天告警, 	您可在下方修改时间范围。				
2025-04-12 11:22:06 ~ 2025-04-18 11	:22:06 📋			告誓ID: a	۵ ۵
告警ID	告讐时间	告警类型 🔽	告警级别 ⑦	聚合次数	操作
al	2025-04-18 10:07:42	审计风险	高风险	1	洋情
共1条				10 ∽ 条/页 1	/1页 ▶ ⊨



() 说明:

- 1. 对于审计风险、模型风险、自审计风险,会跳转到**告警历史**页面,方便您进行告警处置。
- 2. 对于 Agent 掉线风险,会跳转到 Agent 管理页面,您可重新进行 Agent 部署。
- 3. 对于 QPS 超限风险、存储超限风险,会跳转到概览页面,您可查看当前 QPS 和存储情况。



告警设置

最近更新时间: 2025-05-26 18:00:23

触发告警时,数据安全审计会根据配置的告警规则向指定用户发送告警通知。

 说明: 支持微信,站内信,邮件接收告警通知。

前提条件

已开启事件告警通知,详情请参见 消息订阅管理。

操作步骤

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击系统管理 > 告警管理。
- 2. 在告警历史页面,单击**告警设置**,进入告警设置页面。
- 3. 在告警设置页面,可按告警类型/等级设置告警时间。
 - 告警聚合设置:为应对告警风暴,您可以通过设置实时告警数量,将一小时内超过阈值的多个告警事件进行聚合通知。
 - 配置告警条件:根据审计规则和策略,配置相应的告警条件,单击告警开关 🔵 即可开启或关闭相应策略的告警通知。
 - 设置告警时间:根据实际需要,设置告警的时间范围和频率,默认全天告警,同时可进行接收通知时间范围的自定义配置。

告警察合设置						
告警聚合开关						
实时告警数量	- 3 +					
	1小时内,同一告誓类型触发的告誓消息前3%	次实时发送,从第4次开始	进行消息聚合			
审计风险告警						
告警风险等级	告警时间				告警开关	
高风脸	○ 全天告警	〇时间	选择时间	٢		
中风险	○ 全天告警	()时间	选择时间	0		
低风险	○ 全天告警	〇时间	选择时间	0		
行为模型告警						
告警风险等级	告警时间					
高风脸	○ 全天告警	〇时间	选择时间	0		
中风险	○ 全天告警	〇时间	选择时间	٢		
低风险	○ 全天告警	〇时间	选择时间	Ø		
自审计告警						
告警风险等级	告警时间					
高风险	○ 全天告警	〇时间	选择时间	0		
中风险	○ 全天告警	〇时间	选择时间	٢		
低风险	○ 全天告警	〇时间	选择时间	Ø		
其他告警						
Agent撞线	 全天告警 	〇时间	选择时间	٢		
QPS超出规格限制	○ 全天告警	〇时间	选择时间	Q		
存储空间不足	○ 全天告警	〇时间	选择时间	Ø		

▲ 注意

• 请确认消息订阅中"告警消息-安全告警通知"已打开,进入 消息订阅页面 设置。

• 同一操作触发的告警消息超过设定的阈值时,超出阈值的告警信息将会聚合发送。



Agent 管理

最近更新时间: 2025-05-26 18:00:23

Agent 部署

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击系统管理 > Agent 管理,进入 Agent 部署页面。
- 2. 在 Agent 部署页面,根据数据资产添加位置,提供下载链接。配置步骤以及配置注意事项,详情请参见 Agent 部署。
- 3. 在 Agent 部署页面,分为腾讯云内网 Agent 和 腾讯云外 Agent。
- 腾讯云内网 Agent

数据资产为腾讯云内资产(关系型云数据库、NoSQL 云数据库、企业分布式云数据库、自建数据库),优先选择 Linux 在线部署,同时也可选择下载 Linux Agent 或下载 Windows Agent 后进行部署。

Ø	》腾讯云内网Agent
适	用于腾讯云VPC内、或通过专线与腾讯云VPC打通的环境部署。Agent将默认允许采集同一VPC的数据资产流量。
Lir	nux在线部署:Linux操作系统,推荐使用在线部署。
	Linux在线部署 Linux Agent Linux Agent

腾讯云外 Agent

数据资产为腾讯云外资产(腾讯云外数据库)。即可下载 Linux Agent 或下载 Windows Agent。

()	为保障网络安全	全,需要开通白谷	名单,腾讯云外Agent	才能正常上报流	建。请联系客服 物	助开通。		
⊕ #	腾讯云外Age	nt						
适用于	于通过腾讯云外	且未与腾讯云VF	PC打通的环境部署,如	D:其他云、ID	C。Agent将默认	心许采集腾讯云	外的数据资产流量	1
Linux	(在线部署: Lin	ux操 <mark>作系统,推</mark>	荐使用在线部署。					
Li	inux在线部署(即将上线)	🛃 下载Linux Age	ent 🛃 下	載Windows Agen]		

Agent 列表

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击系统管理 > Agent 管理,进入 Agent 部署页面。
- 2. 在 Agent 部署页面,单击 Agent 列表,进入 Agent 列表页面。
- 3. 在 Agent 列表页面,可以查看所有已配置成功的 Agent。Agent 列表默认展示内容包括: 部署 IP、部署位置、VPC、地域、操作系统、机器负载、最后上

Agentatia Agentati	180								
全部基督在五	· © 28764 - 2872^								NAAREPEER Q Q
部務で	部署位置	VPC	1816	操作系统	8.810.00	最后上报时间	送行状态 Y	开启状态	¥i-f7
-	8857	-		linus	CPU: 0% PSG: 0%	2024-11-13 14:57:54	• 已進出		1242 1012 BOD
	將設立內國		CH.	linas	CPU: 0% (\$98): 0%	2024-10-09 15:34:02	• 已腐然		NUTE 1018. MIN
	腾讯元内阁	-	CH.	linus	CPU: 0%	2023-08-13 09:03:55	 已高线 		1010 1010 BID

报时间、运行状态、开启状态及相关操作。

4. 在 Agent 列表页面,您可以按部署位置、地域、数据资产、部署 IP、运行状态对 Agent 进行搜索。

gont왕왕 Agent카용	<u>i</u>								
全部神著位五	- © 28588 - 2857-	×							NAARENER Q Q
部務中	部署位置	VPC	1618	操作系统	机器负载	编码上程时间	油行状态 Y	开启状态	38-07
10100-001	腾讯元外		-	linux	CPU: 0% (4)\$2: 0%	2024-11-13 14:57:54	• 已高级		SNE 1012 BNR
	教机力内间	-	г°н	linux	CPU: 0% PSW: 0%	2024-10-09 15:34:02	• CAR		6251 2011 85 8
	普讯五内周	-	гн	linux	CPU: 0% /982: 0%	2023-08-13 09:03:55	• 已高级		5241 2012 800

5. 在 Agent 列表页面,选择所需部署 IP,单击编辑,可以查看和修改 Agent 配置相关信息。

🕛 说明



设置停止审计阈值。为尽最大可能保证业务运行不受影响,您可以设置基于 CPU 与内存使用率的阈值,当 Agent 宿主机性能超过阈值时,Agent 并暂停流量采集,待宿主机性能降回阈值以下时再恢复采集。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。

编辑Agent						×
* 超过阈值停止审计:						
* CPU利用率: 80 %	* 内存利用率:		80	%		
 实例ID/名称 数据资产名称 	数据资产类型	VPC		数据资产IP	地域	
	MySQL				广州	Î
	SQL Server					
	MySQL				重庆	
)	MySQL				重庆	
共 12 条			10 ▼ 条/页		1 /2页 🕨	H
	确定	取消				

6. 在 Agent 列表页面,选择所需部署 IP,单击卸载 > 确定,等待卸载完成后,单击删除即可删除该部署 IP。

全部流量来源 ▼	全部地域 * 全部资产					
	貫讯云内网					
	腾讯云外			2021-12-17 16:29:02		
	展讯云内网		×	2021-12-17 16:30:11		
	腾讯云内网	确定卸载该Agent?		2021-12-17 16:30:34		
	腾讯云内网	歌迎	現石油	2021-12-17 16:30:26		



网络管理

最近更新时间: 2025-05-26 18:00:23

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**系统管理 > 网络管理**。
- 2. 在 VPC 通道列表中,显示 VPC、地域、VIP(Virtual IP)、添加类型、关联数据资产数量和部署 Agent 数量。

网络管理						
VPC通道列表						
本列表的您展示通过PrivateLink线 开启VPC中数据资产的审计权限的	术与数据安全审计服务建立连接通道的VPC 1,将自动建立数据安全审计服务到该VPC的	、Agent臺北該臺蘆將采集的數媒率流量上投 遺道,您也可以自主承加及管理。	到数据安全审计服务。			
10 1 0						
VPC	地域	VIP	类型	关联数据资产数量	部署Agent数量	操作
	使云		自动添加			删除

3. 如需具体查看同一 VPC、地域下的关联数据资产,单击关联数据资产数量栏下的数字,即可查看。

添加						
VPC	地域	VIP	类型	关联数据资产数量	部署Agent数量	操作
vi	广州		关联数据资产信息			删除
vı	广州		数据资产名称 资产来源	数据资产类型	IP	删除
vı	广州		自建数据库	MySQL		删除
vı	<i>r</i> ∸ ₩I		自建数据库	MySQL		翻除
vį	广州		自建数提库	Redis		删除
vı	广州		自建数据库	MongoDB		翻除
vj	广州		自建数据库	Oracle		删除
vı	广州		共 5 条			删除
v	广州		自动添加	5	9	删除

4. 用户可自主添加新的 VPC 通道列表。单击添加,即可弹出添加 VPC 通道弹窗。

添加VF	PC通道	×
0	将在所选子网下创建名称以"DSAudit_" 开头的终端节点,并占用一个IP地址	×
* 地域:	⑤ 请选择	Ŧ
* VPC:	请选择	Ŧ
* 子网:	请选择	Ŧ
	确定取消	

5. 选择对应的地域、VPC 和子网 IP,单击确定即可完成添加。添加完成将在所选子网下创建名称以"DSAudit_"开头的终端节点,并占用一个 IP 地址。
6. 某些 VPC 通道若不再需要,可单击操作列的删除,经二次确认后,即可销毁该 VPC 通道。

() ไ ∄	礼明 削除后,将无法采集部	署在该 VPC 的 A	Agent 流量。该 VI	PC 内的数据资产将	无法审计。	
VPC	地域	VIP	类型	关联数据资产数量	部署Agent数量	操作
vpc	/**#I		手动添加	0	0	899
vpc	广州		手动添加	0	0	翻除
vpc-	广州		手动添加	0	0	8 59



自审计

最近更新时间: 2025-05-26 18:00:23

检索操作日志

操作日志负责审计数据安全审计账户的操作,能够浏览账户操作日志列表并对行为规则进行配置。

1. 登录 数据安全审计控制台,在左侧导航栏中,单击**系统管理 > 自审计**,进入操作日志页面。

2. 在操作日志页面,您可以根据行为分类、操作时间、操作账户、操作 IP 检索查看操作完整信息。

全部行为分类 * 改和订约	(1581-51)		消益入却作用の小月前の の日本の対応はつけてい	٩٥
操作时间 0	操作程户	Nettup:	行为分类 新作用CP	操作行为
2025-02-06 16:08:36	1000000		新作P 要计例如检查	带计风险列表资料
2025-02-06 16:06:42	1000000		审计概范	消益等计概点页
2025-02-08 15:59:22	1000000		审计概克	湖京市计概定页
2025-02-08 15:58:22		10000	Agent的表情理	查與AgantH表

行为规则配置

() 说明

- 1. 登录 数据安全审计控制台,在左侧导航栏中,单击**系统管理 > 自审计**,进入操作日志页面。
- 2. 在操作日志页面,单击行为规则配置页签,进入行为规则配置页面。
- 在行为规则配置页面,显示行为操作、行为分类、告警模板、备注、危险等级及是否开启告警。您可根据行为分类、行为操作及危险等级搜索查看相关配置信息。

所有	数据由系统内建生成	. 用户可以根据需求讲行修改。

全部行为	v 全部操作 v 全部操	φ			
行为操作	行为分类	告誓模版	备注	危险等级	是否开启告警
Agent下载	Agent下較部署	1	/	低风脸 マ	
Agent就量部署	Agent下數部書	1	1	任风险 *	

字段说明:

- 行为操作:用户对系统各个账户的功能操作。
- 行为分类:用户对系统功能操作所属的模块名。
- 告警模板:用户执行操作时邮件所发送的告警内容,单击 ≥ ,可修改告警模板。
- 备注:用户对行为规则的进一步说明,单击 ,可修改备注说明。
- 危险等级:对用户操作行为的评级,可设置行为危险等级,包括低风险、中风险及高风险。

○ 是否开启告警:单击 ◯ 开启后,触发行为规则审计,则会发送告警信息,单击 ◯ 关闭后,只会记录操作,不会发送告警信息。



数据安全审计传统型 v5.1.0 系统管理 系统资源监控

最近更新时间: 2021-09-28 11:13:36

以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击**系统资源监控**,即可进入资源监控页面,该页面包括系统详细信息、系统存储空间统计和 流量走势实时统计。

系统详细信息

系统详细信息包含系统产品名称、系统版本、产品规格、已用/总数据资产数、连续运行时长、购买峰值流量、系统当前时间参数信息。

系统详情						系统当前时间 2021-08-13 15:48:40
产品名称	V5.1.0	里启				
oC	合规版 ^{产品规格}		3/3 个 已用/总数据资产	 3000 QPS 购买峰值流量	6	0年0月8日 19小时53分24秒 海峡运行时长

系统存储空间统计

存储空间统计用于展示数据安全审计实例当前的存储状态。在系统存储空间统计右上角,单击**清理剩余空间**,将清理的数据包含所选的日期。例如,选择了12月1 日至12月3日,则会删除12月1日、2日、3日,3天的数据。



- 系统占用空间:数据安全审计自身代码所占存储空间;
- 审计日志占用空间:数据安全审计记录的数据库操作信息日志占用空间;
- 其他占用空间:数据安全审计实例其他代码、配置文件占用空间。



流量走势实时统计



流量走势实时统计能统计一定时间跨度(最近 30 分钟、最近 24小时、最近 7 天)内数据安全审计中所审计的所有数据库的 QPS,确认全网 QPS 峰值是否超 过购买峰值,以帮助管理员了解数据安全审计性能状况,及时扩容升级产品。

流量走势实时统计(QPS)	最近30分钟 最近24小时 最近7天
3	
2.5	A
2 2021-08-11 15:49:02 QPS 1	\wedge
1.5	
0.5	
2021-08-11 15:47:04 2021-08-11 15:53:03	2021-08-11 16:02:03 2021-08-11 16:08:03



用户管理

最近更新时间: 2025-05-29 09:43:32

以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中单击用户管理即可进入用户页面。

查看账号信息

账号管理用于管理 DSA(Data Security Audit)实例所有账号。系统管理员可以通过列表查看所有账号信息,包括所属角色、真实姓名、创建日期以及联系 方式等。

() 说明

- 密码有效期为90天,密码规则如下所示:
- 密码长度:在12-20位字符数以内。
- 复杂度:至少包含以下 3 类字符 小写字母(a-z)、大写字母(A-Z)、数字(0-9)、特殊符号(~!@#\$%^&*()_+-=|{}[]:;'<>,.?)。
- OTP(One-Time Password) 二维码:如需开启 OTP 实现登录双重验证,可在相应账号右侧操作栏,单击 OTP二维码,或在数据安全审计管 理页面右上角,找到管理员账号下的 OTP 验证,单击 OTP二维码,查看原图并扫描动态校验码。

帐号名称	所雇角色	平 真实姓名		创建人	最后修改人	最后修改时间	联系方式	登录IP范围	操作
sysadmin	系统管理员		2020-09-28 10:00	系统默认创建	7	2020-10-20 16:52	电话: 邮稿: 微信:	洋橋	OTP二维码 编辑
useradmin	审计管理员		2020-09-28 10:00	系统默认创建	/	2020-09-28 10:00	电活: 邮稿: 微信:	详情	OTP二维码 编辑

添加账号

如需要增加管理员账号,单击添加账号,在弹框中填写账号信息,选择所属角色后,单击确定即可。

* 账号:				
* 密码:				
* 真实姓名:				
* 手机号码:				
* 邮箱:				
★ 微信号:				
* 所属角色:	审计管理员		~	
登录IP范围:	起始IP	结束IP	操作	
	0.0.0.1	255.255.255		
	添加 (当ip为ipv6格式时,仅对	(超始)P有效)		
			取消	确定

修改和删除账号

如需对账号进行修改或删除,可在相应账号操作列单击**编辑**或**删除**对账号进行调整。



系统默认创建账号不可删除。

帐号名称	所屬角色	7 真实姓名	创建日期	创建人	最后修改人	最后修改时间	联系方式	登录IP范围	操作
sysadmin	系统管理员		2020-09-28 10:00	系统就认出國	7	2020-10-20 16:52	电话: 邮箱: 微信:	9710	OTP三维码 编辑
useradmin	审计管理员		2020-09-28 10:00	派统就认 创建	7	2020-09-28 10:00	电话: 邮箱: 微信:	¥40	OTP三编码 编辑
sysaudit	操作审计管理员		2020-09-28 10:00	斯纳默认识跟	7	2020-09-28 10:00	电话: 邮箱: 微信:	1941B	OTP三编码 编辑
-	审计管理员	-	2020-11-12 11:45	sysadmin	7	2020-11-12 11:45	电话: 1 邮箱:	1910) 1	OTP二维码 编辑 删除



OTP 设置

最近更新时间: 2025-05-27 16:30:32

本文档将为您介绍如何开启 OTP 校验,并通过 OTP 校验登录数据安全审计管理页面。

操作步骤

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击 OTP 设置,即可进入 OTP 设置页面。



3. 在 OTP 设置页面,设置校验开关,如需开启 OTP 验证选项,选中开启 OTP 验证,出现弹窗,根据提示扫 OTP 码,输入正确的 OTP 码,单击**确定**,退 出登录系统即可。

 说明 建议开启 OTP 验证之前,提前通知各管理员登 	录系统扫描 OTP 验证二维码,避免其无法登录该系统。
OTP设置	
 校验开关:● 开启OTP验证 关闭OTP验证 	
	动态校验码 ×
	身份标识二维码
	密钥:
	请输入您的6位OTPt交验码 取消 翻定



4. 再次登录数据安全审计管理页面,需要输入OTP 校验码。





告警设置

最近更新时间: 2025-01-10 19:17:22

告警支持针对每个审计规则策略进行告警,告警支持邮件告警、syslog 告警、短信告警、企业微信告警,具体操作步骤如下: 1. 登录 数据安全审计控制台,找到需要操作的审计系统,在右侧操作栏,单击<mark>管理</mark>,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击告警设置,即可进入告警设置页面。

```
    说明:
    如忘记登录密码,可以提交工单 找回密码。
```

- 3. 在告警设置页面,分别对告警开关、系统资源告警配置、syslog 告警配置、邮件告警配置、短信告警及企业微信告警功能进行设置。
- 告警开关

```
在告警设置页面,单击告警开关,分为告警方式和告警内容,打开需要开启告警的选项,单击提交,即可对 syslog 告警配置 中所设置的服务器进行监控,且
当满足告警条件时,将触发告警,并发送邮件至您所 配置的告警邮箱 中。
```

```
      ⑦ 税期:

      若需要接收告警信息,需打开邮件告警开关,目已在:邮件告警配置 中设置告警接收邮箱,否则无法接收告警信息。

      任警设置

      查普开关 系统资源告答配置 影yslog告答配置 邮件告答配置 短信告答 企业微信告答

      ● 軟柱配置
      syslog告答配置 邮件告答配置 短信告答 企业微信告答

      ● 軟柱配置
      syslog告答配置 ● 軟体配置

      ● 軟柱配置
      syslog告答

      ● 軟柱配置
      of 水体配置

      ● 軟柱配置
      for manufacter

      ●
      軟柱配置

      ●
      ●

      ●
      ●

      ●
      ●

      ●
      ●

      ●
      ●

      ●
      ●

      ●
      ●

      ●</t
```

• 系统资源告警配置

在告警设置页面,单击**系统资源告警配置**,设置系统资源告警的触发条件,可将磁盘、内存、CPU 负载在0 – 100%之间调整,可自定义带宽值,单击**提交**, 即可对 syslog 告警配置 中所设置的服务器进行监控。



告警设置							
告警开关	系统资源告	警配置	syslog告警配置	邮件告警配置	短信告警	企业微信告警	
	磁盘:	0 %	25 %	50 %	75 %	0 100 %	% (超过设定数值后将触发告答)
	内存:	0 %	25 %	50 %	75 %	100 %	% (超过设定数值后将触发告答)
	CPU负载:	0 %	25 %	50 %	75 %	100 %	% (超过设定数值后将触发告答)
	带宽:	_	10 + MB (超过)	设定数值后将触发告警)			
_							
保存							

syslog 告警配置

▲ 注意: 目前 syslog 告警服务只支持 TCP 协议。

在告警设置页面,单击**syslog 告警配置** ,输入需要记录的 syslog 服务器 IP 和端口,单击**提交**,即可完成 syslog 告警条件配置,设置完成后将监控所配 置的服务器 。

告警设置							
告警开关	系统资源告警	翻置	syslog告警配置	邮件告警配置	短信告警	企业微信告警	
() 目前sy	/slog告警服务只支	持tcp					
	syslog服务器. *	请输入sysl	og服务器				
	端□ *	— 22 俞入范围限制	2 + J1-65535				
保存	测试						

• 邮件告警配置

单击**邮件告警配置**,依次填入邮件服务器的相关配置信息,如需添加多个收件人,请以英文分号分隔,填写完成后,单击**提交**,当满足告警条件时,将发送邮 件至所配置的邮箱中。

说明:
 若填写 QQ 邮箱账号,密码需填写所设置的邮箱密码。



告警设置			
告警开关	系统资源告	警配置 syslog告警配置 邮件告警配置 短信告警 企业微信告警	
	SMTP服务器: *	第二方邮件服务容易受服务器反位现机制影响。如课到不可用的、建议学试切换其他邮件服务	
	谎口:*	- +	
	邮件账号:*		
	密码:*		
	发件人:*		
	收件人:*		
	TLS:	※「NKI牛人頃以方亏; 万裕	
保	存测试		

• 短信告警设置

单击**短信告警**,依次填写短信告警设置相关配置信息。如需添加多个手机号,单击添加,填写完成后,单击**保存**,当满足告警条件时,将发送信息至所配置的



	邮件告警配置	短信告警	企业微信告警	
能使用腾讯云短信SMS,请自主开通	,并在本页面完成配置。			
请输入SecretId				
请输入SecretKey				
请选择地域				v
请输入下发手机号码				添加
请输入SdkAppId				
法输入效久				
123 CT H				
请输入模版ID				
请输入发送间隔	分钟			
	能使用勝讯云短信SMS,请自主开通 请输入SecretId 请输入SecretKey 请输入SecretKey 请输入SecretKey 请输入SecretKey 请输入SecretKey 请输入SecretKey 请输入SecretKey	 能使用勝讯云短信SMS,请自主开通,并在本页面完成配置。 请输入SecretId 请输入SecretKey 请输入下发手机号码 请输入SdkAppId 请输入签名 请输入使送间隔 分钟 	能使用購讯云短信SMS,请自主开通,并在本页面完成配置。 请输入SecrettKey 请输入StecretKey 请输入SdkAppId 请输入然名 「清输入燃気 「清輸入燃気	 編成入Secretid · · ·

单击**企业微信告警**,填写相关配置信息,单击**保存**,当满足告警条件时,将发送信息至所配置的企业微信中。

告警设置						
告警开关 系统	资源告警配置	syslog告警配置	邮件告警配置	短信告警	企业微信告警	
说明: 请在P	C版企业微信需要错	5警的群里添加群机器人,	将WebHook地址填写在	本页面。		
WebHoold也	业: * 请输入W	ebHook地址				
保存	测试					



备份服务器设置

最近更新时间: 2025-05-27 16:30:32

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击备份服务器设置,即可进入备份服务器设置页面。

① 说明	
如忘记登录密码	3,可以 提交工单 找回密码。

 在备份服务器设置页面,依次输入备份服务器地址、备份服务器端口、备份服务器用户名、备份服务器密码、备份服务器目录路径,打开备份开关,单击保存 即可完成备份服务器设置。

🕛 说明

- 备份服务器地址需为公网 IP 地址,并且入站安全组是放通状态,详情请参见 添加安全组规则 。
- 备份服务器通过 SSH 的方式进行备份,备份服务器设置成功后,系统每日02:00(UTC+8)定时备份前一天的数据到目标机器目录。

备份服务器设置	
备份服务器设置 数据	灰复
备份服务器地址:*	
督份服务器端□:*	- 22 +
备份服务器用户名:*	root
备份服务器密码:*	*****
备份服务器目录路径:	
备份开关:	
保存测试	

- 4. 设置完成后,数据安全审计管理系统中的数据将会按照设置路径进行备份。
- 5. (可选)如需恢复之前存在的数据,在备份服务器设置页面,单击**数据恢复**页签。



6. (可选)在数据恢复页签中,单击**数据恢复**,选择恢复日期并导入恢复数据即可。

数据恢复					×
恢复日期:	选择日期	Ħ	备份文件:	点击上传文件	
		关闭			

审计管理 安全审计与分析 审计数据

最近更新时间: 2025-05-27 16:30:32

审计概览

- 1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面,详情可参见 控制台登录。
- 2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择**安全审计与分析 > 审计概览**,即可进入审计概览页面。
- 在审计概览页面中,可总览全网数据库日志信息,态势分析,风险占比以及查询单个数据库资产详细信息,如需了解数据库资产审计详细内容,可在审计概览 页面下方查询详细信息。
 - 日志总数:用于统计全网各数据资产日志总数。
 - 今日日志:用于统计全网各数据资产今日日志总数。
 - 今日风险:用于统计全网各数据资产今日风险总数。
 - 今日会话:用于统计全网各数据资产今日会话总数。
 - 态势分析:可查看您所配置的审计单元的审计趋势,风险趋势,会话趋势,还可按照高风险、中风险、低风险进行查看各个风险级别详细数据,每个报表 可展示三种走势图及三类风险级别数据:
 - **审计趋势**:用于展示数据资产的审计单元语句压力,展示时间有24小时、7天、30天。
 - 风险趋势:用于展示数据资产的审计单元高中低三类风险的统计信息,展示时间有24小时、7天、30天。
 - 会话趋势:用于展示数据资产的审计单元各类会话信息,展示时间有24小时、7天、30天。
 - 风险占比统计:用于显示数据资产对应的命中风险等级。
 - 风险等级:用于展示数据资产审计单元有关的自定义规则命中风险信息,展示时间有24小时、7天、30天。
 - 数据资产:用于展示被命中的数据资产,展示时间有24小时、7天、30天。
 - 资产审计:主要展示单个数据资产的会话总数,DDL 操作数量、失败会话数量、最大并发会话及风险数等信息。

日本品数 30.35万款 已运行 0 年 3 天 22 小时 空间时间: 系统者: 15.56 / 5056 数据者: 1.5768 / 19768	ФВВак 8.34 Бак Вяны: 74% ▲ Яяны: 183% ▲	今日风险 0↑ 日环比:0%▼		周环比: 0%▼	今日会请 1.15万次 日环北: 92%▲	MERLE: 680% 🔺
恣势分析 24小时	7天 30天 2021-03-10 ~ 2021-03-16 日	风险占比统计		24小时	7天 30天 202	21-03-10 ~ 2021-03-16 🗇
审计趋势 风险趋势 会活趋势		风险等级	数据选产			
			63R 7562		■ 50) - 700) - 600 (276 263 0

日志检索

日志检索主要提供日志查询与导出功能。

- 1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面,详情可参见控制台登录。
- 2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择**安全审计与分析>审计日志**,即可进入审计日志页面。
- 3. 管理员通过 审计概览 定位到疑似有风险的数据资产,或者企业网络已经发生数据库安全问题时,可在日志检索页面查询并导出日志信息。

审计日志	全部数据资产	v					
最近一小时	今天 昨天 7	(周 上周 本月 上月)	自定义 高级铸造 v				
0 1	闻已完成,数据总量: 141201条						
序号	用户答	客户请IP	时间 \$	命中规则	风险等级 \$	SQL语句	操作
1		1	2021-08-13 13:49	ş	低稅	-	详情
2		1	2021-08-13 13:49	1	低危	01	详情

日志查询



Ŧ

查看数据详情

腾讯云

在日志列表中,可单击某条记录查看其详细内容。

审计日志详情		>
基本信息		
操作语句		
操作英型		
操作时间	08-05 14:38 46	
SessionId		
命中规则		
风险等级	46风险	
数据库		
数据库IP		
数据库用户		
详细信息		
表名		
影响行数		
执行时间		
返回消息		
诚回码		
客户端P		
包长度		
使用工具		

日志导出

检索出需要导出的数据,现已支持不限数量导出,在列表上方单击 上,弹出导出数据弹窗,单击**确定**即可将数据导出,导出文件类型为 Excel(.xlsx格式)。









规则配置

最近更新时间: 2025-05-27 16:30:32

规则配置页面可配置触发风险告警的命中规则。数据安全审计已提供17个内置规则,可满足大多数安全场景,内置规则不可删除、不可编辑。您也可以根据业务 需要,添加自定义规则,下面将为您详细介绍配置操作。

操作步骤

以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中,选择**安全审计与分析 > 规则配置**即可进入规则配置页面。

新建规则

如需自定义规则满足个性化审计需求,单击**添加规则**,进入新建规则页面,填写规则名称等,单击**保存**即可。

△ 注意

- 规则配置支持同一规则配置多个条件,多个条件之间为 "与"关系,必须全部匹配才能够触发规则和告警。
- 自定义规则默认为黑名单,触发后将产生告警并且记录入库。如果管理员需要节省数据安全审计的审计单元的存储空间,指定部分操作行为不记录不 入库,可在规则中指定相关操作后,选择"白名单"选项,并且将告警选项都取消。

以上操作完成后,即可实现白名单类型规则配置,减少误报、减轻数据安全审计的审计单元存储压力。

• 规则示例

在规则配置页面,单击添加规则,按下图配置规则,表名和阈值根据您的业务场景自行设定,单击保存即可。



添加规则					
基础信息					
规则类型	● 黑名单 (○ 白名単			
* 规则名称	请输入规则	名称			
规则备注	请输入规则	备注			
风脸等级	• 低风险 (○ 中风险 ()	高风	场	
规则定义					
客户端	客户端IP	包含	\sim	可配置多个IP,英文逗号分隔,如:192.168.1.1,19	添加
服务端	数据库IP	包含	\vee	可配置多个IP, 英文逗号分隔, 如: 192.168.1.1,19	添加
	数据库端口	大于等于	\sim	请输入数据库端口,范围1-65535	添加
	数据库用户	包含	\sim	可配置多个用户,英文逗号分隔,如:sys,root.sys	添加
	数据库名	包含	\sim	可配置多个数据库名,英文逗号分隔,如:mysql.t	添加
行为	操作类型	包含	\vee	select	添加
	操作语句	包含	\vee		添加
	表名	包含	\sim	xx_test	添加
语句执行	执行时长	大于等于	\vee	请输入数值,取值范围0-9999	添加
	影响行数	大于等于	$^{\vee}$	50 行	添加
时间限制	操作时间	大于等于	\sim	请选择日期	添加

• 规则配置建议

以下三个建议规则仅作为示例,用户可根据自身业务自行配置。



○ 防爬取规则:防止使用例如 select 操作语句,爬取表数据。

添加规则					2
基础信息					
规则类型	● 黑名单) 白名単			
* 规则名称	请输入规则	名称			
规则备注	请输入规则	备注			
风脸等级	● 低风险	()中风险 (高风	脸	
规则定义					
客户端	客户端IP	包含	~	可配置多个IP,英文逗号分隔,如: 192.168.1.1,19	添加
服务端	数据库IP	包含	\sim	可配置多个IP, 英文逗号分隔, 如: 192.168.1.1,19	添加
	数据库端口	大于等于	\sim	请输入数据库端口,范围1-65535	添加
	数据库用户	包含	\sim	可配置多个用户,英文逗号分隔,如:sys.root.sys	添加
	数据库名	包含	\sim	可配置多个数据库名,英文逗号分隔,如:mysql.t	添加
行为	操作类型	包含	\sim	select	添加
	操作语句	包含	\sim		添加
	表名	包含	\sim	请输入表名,多个用英文逗号隔开	添加
语句执行	执行时长	大于等于	\sim	请输入数值,取值范围0-9999	添加
	影响行数	大于等于	\sim	100 行	添加
时间限制	操作时间	大于等于	\sim	请选择日期	添加

▲ 注意

影响行数可以根据业务自行配置。



○ 慢查询发现规则:检查执行时间较长的 SQL 语句,便于进行优化。

规则类型	● 黒名单 (白名单			
规则名称	请输入规则:	名称			
规则备注	请输入规则	备注			
风险等级	 低风险 	○ 中风险		現金	
则定义					
客户端	客户端IP	包含	~	可配置多个IP, 英文逗号分隔, 如: 192.168.1.1,19	添加
服务端	数据库IP	包含	$^{\vee}$	可配置多个IP,英文逗号分隔,如: 192.168.1.1,19	添加
	数据库端口	大于等于	\sim	请输入数据库端口,范围1-65535	添加
	数据库用户	包含	\vee	可配置多个用户,英文逗号分隔,如:sys,root,sys	添加
	数据库名	包含	V	可配置多个数据库名,英文逗号分隔,如:mysql.t	添加
行为	操作类型	包含	\vee	select	添加
	操作语句	包含	\vee		添加
	表名	包含	\vee	请输入表名,多个用英文逗号隔开	添加
语句执行	执行时长	大于等于	\sim	500 堂秒	添加
	影响行数	大于等于	~	请输入数值,取值范围0-9999	添加
时间限制	操作时间	大于等于	\sim	请选择日期	添加

执行时间可以根据业务自行配置。

○ 危险操作规则:检查执行 DELETE/DROP/ALTER 等类型的高危 SQL 语句。

印规则					
础信息					
规则类型	◉ 黑名单) 白名单			
* 规则名称	请输入规则	名称			
规则备注	请输入规则	备注			
风险等级	● 低风险	○ 中风险		场	
则定义					
客户端	客户端IP	包含	\vee	可配置多个IP, 英文逗号分隔, 如: 192.168.1.1,19	添加
服务端	数据库IP	包含	\sim	可配置多个IP, 英文逗号分隔, 如: 192.168.1.1,19	添加
	数据库端口	大于等于	\sim	请输入数据库端口,范围1-65535	添加
	数据库用户	包含	\sim	可配置多个用户,英文逗号分隔,如:sys.root.sys	添加
	数据库名	包含	\sim	可配置多个数据库名,英文逗号分隔,如:mysql,t	添加
行为	操作类型	包含	\sim	drop	添加
	操作语句	包含	\sim		添加
	表名	包含	\sim	请输入表名,多个用英文逗号隔开	添加
语句执行	执行时长	大于等于	\sim	请输入数值,取值范围0-9999	添加
	影响行数	大于等于	\sim	请输入数值,取值范围0-9999	添加

修改规则

🔗 腾讯云

在规则列表中,找到需要修改的规则,在右侧操作栏中,单击**编辑**,修改信息后单击**保存**即可。

规则列表 规则定用						
+ 2002 C 800 2070	明和武士					
规则名称	规则类型	规则属性	风险等极	关联数据统产	備注	現作
201EIA	白名単	内震规则		全部	系统内置规则	编辑
CVE引擎	白石単	内置规则		全部	系统内置规则	编辑
3 86654831	黑名单	日定义规则	82			浦祖 翻除

删除规则

在规则列表中,找到需要删除的规则,在右侧操作栏中,单击**删除**,再单击询问窗**确定**即可。

現到列表 現到雇用						
+ 湖川市 合語 治体の引起素						
10(65	1701040	1551年19	网络等级	半副新振动 声	9/ 1	10/11
AI引擎	白石単	内置規则		全部	系统内置规则	etri B
CVE引擎	白谷单	内置规则		全部	系统内置规则	 2% 前以要服除吗?
26/2021	展亮单	目中心探引	**	Concerning and the second		00x8 (F0)
	100-0-	EALCORG .	1803			



审计报表

最近更新时间: 2025-01-10 19:17:22

审计报表功能主要展示所有配置过的审计组数据,并提供搜索、查看及 PDF 下载功能,具体操作步骤如下: 1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择**安全审计与分析 > 审计报表**,即可进入审计报表页面。

说明 如忘记登录密码,可以提交工单找回密码。

3. 在审计报表页面中,可查看内容包括报告名称、报告说明及发送目标等字段,同时可以进行相关操作,每个页面默认展示20条数据,可按照报告名称、生成方 式、开始时间及结束时间,对报告进行搜索,还可下载 PDF 报告。

新建設表				2021-07-31 00:00 ~ 2021-08-13 23:5	9 📩 输入报表名称 Q	
报表名称	报表说明	发送目标	报表生成时间	报表类型	状态 ▼	操作
定时_2021-08-12	定时八点半	s	2021-08-12 20:30:00	周期报表	⊘ 已生成	查看 pdf下载 删除
定时_2021-08-11	定时八点半	S	2021-08-11 20:30:00	周期报表	⊘ 已生成	查看 pdf下载 删除
定时_2021-08-10	定时八点半	s	2021-08-10 20:30:00	周期报表	⊘ 已生成	查看 pdf下载 删除

• 定时生成报表

数据安全审计管理系统支持定时生成报表。

在报表上方单击**新建报表**,弹出新建报表弹窗,选择"周期报表",并依次输入模板名称、重复周期(可选择定时执行、每天、每周、每月)、执行时间(精 确到时分秒)、报告说明,设置完成后,单击**确定**,即可在您设定的执行时间定时生成报表。

新建报表					×	P 4
报表类型:	🔵 即时报表	● 周期报表				
报表名称:*	定时					
重复周期:	每天	,	•	20:30:00	()	
报表说明:*	定时八点半					
					5	
	确定	目の消	当			

• 即时生成报表

数据安全审计管理系统支持即时生成报表,即生成某个时间段内的报表。

在报表上方单击**新建报表**,弹出新建报表弹窗,选择"即时报表",依次输入报告名称、包含资产、时间选择、报告说明,单击**确定**,即可输出您规定的时间 范围内的报表。

注意开始时间应早于结束时间。



新建报表		×
报表类型:	● 即时报表 周期报表	
报表名称:*	请输入报表名称,最多64字符	
包含资产:	请选择 🔻	
时间选择:*	选择时间	
报表说明: *	请输入报表说明,最多256字符	
	0 / 256	
	确定 取消	



数据资产与 Agent

最近更新时间: 2025-05-27 16:30:32

Agent 下载

- 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,即可进入审计用 Agent 页面。
- 2. Agent 部署。在审计用 Agent 页面,选择 Agent 下载 > 添加,可配置审计 Agent 的各类参数并提供下载链接,配置步骤以及配置注意事项,请参见 Agent 部署。
- 3. 添加完成 Agent 后,在 Agent 配置页面,可查看所有已正确安装且能实现 DSA (Data Security Audit)实例网络互通的 Agent 信息。

AgentiltE				
Agent Fitt Agent Fitt				
16.01				
AgentER	第1十個的 (BDP)	#11885#D	R364×	1915
		7000		Tax + date
arms		7000	(1)	782 * 809
共 2 条				10 + 条/页 + + 1 /1页 > +

列表各字段含义如下:

- Agent 名称:用于配置该 Agent 的名称。
- 审计服务 IP: Agent 回传数据的源 IP。
- 审计服务端口: 该 Agent 配置的审计端口。
- 数据库资产:可查看该 Agent 审计的数据库的所有 IP 地址。
- 操作:用于下载该 Agent 的链接。
 - 在右侧操作栏,选择下载 > 下载 Linux Agent或下载 Windows Agent, 弹出部署 IP 窗口, 单击确定即可开始下载 Agent。

△ 注意

- ◎ 若部署机器操作系统 CentOS 版本号小于7 或者 Ubuntu 版本号小于11,必须勾选下方说明,否则无法部署 Agent。
- 请添加安装包需要部署机器的 IP 或 IP 列表。
- 如未添加 IP 信息却部署了会导致 Agent 无法启动。
- 如有新的机器要部署请重新下载安装包并填写机器的 IP 信息。

部署IP	Х
部署机器操作系统centos版本号小于7或者ubuntu版本号小于11(部署机器操作系统centos版本号小于7或者ubuntu版本号小于11,必须勾选此选项 无法部署agent)	(注: 若 页, 否则
取消	确定

○ 在右侧操作栏,选择**下载** > Linux 批量部署,输入部署地址,支持按 IP 或按 IP 段部署,支持添加多行,输入服务器 IP 、SSH 端口号、用户 名、密码,输入完成后单击确定即可。



linux批量部署						×		
部署地址: 部署地址: ubuntu 版本号 按IP部署 接	/data/dbAudit/ 操作系统centos版 小于11,必须勾选成 印段部署	本号小于7 或者ubi ^{起页,} 否则无法部署ag	untu 版本号小于11 (jent)	主: 若部署机器操作系统	centos版本号小于7	或者		
服务器IP		SSH端口号	用户名 root	密码	ø	操作		
添加一行 注: ①SSH的账号密码服务器不会保存只做下发服务使用 ②SSH端口号默认22、用户名默认root,可自行修改								
					取消	确定		

○ 在右侧操作栏,单击删除,可删除该条 Agent 信息。

Agent 列表

- 1. 以 useradmin 账号登录数据安全审计管理页面,在左侧导航栏中,选择审计用 Agent > Agent 列表,即可进入审计列表中。
- 2. 在审计列表中,可以查看所有已配置的 Agent。Agent 列表默认展示内容包括:Agent 名称、部署 Mac、部署 IP、操作系统、部署时间、最新上报时间、 运行状态、开启状态及相关操作。
 - 搜索: 您可以按数据资产、Agent 状态、Agent名称、IP、对 Agent 进行搜索。
 - 查看 Agent 配置详情:在"操作"栏中,单击编辑,可以查看 Agent 配置相关信息。
 - 相关操作:在右侧操作栏,可以对 Agent 进行启动、停止、编辑、卸载、删除的相关操作。

Agent管理								
Agent下载 Agent列表								
全部资产								能入Agent名称考察P C
Agent 858t	NS Mot	15回 IP	19/1:35/32	新型 目	最新上级时间	(6行秋念 ¥)	开始状态	19/s
	5		windows	2021-08-09 17:30:00	2021-08-13 15:44:02	0 217P		
	5	100	Inux	2021-08-04 20.05:09	2021-08-13 15:43:44	0 259		
共 2 条							10 -	④/页 × ← 1 /1页 > ×



操作日志管理

最近更新时间: 2025-01-10 19:17:22

操作审计员负责审计数据安全审计各管理员的操作,防止其他管理员滥用职权进行非法操作。用操作管理员账号登录后,能够阅览管理员操作日志列表并对行为规 则进行配置。

日志检索

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以操作管理员账号登录操作日志页面,在左侧导航栏中单击**行为规则配置**,即可进入操作日志页面。

() 说明		
如忘记登录密码,可以 提交工单 找回密码。		

3. 在操作日志页面,您可以根据操作事件、操作 IP、行为分类、操作时间检索还原非法操作完整信息。

操作日志						
全部行为分类	▼ 选择时间		ti i		请输入操作账户	请输入操作IP
全部行为分类 用户登录	Î	操作账户	直实姓名	操作IP	行为分类	操作行为
用户注销 系统资源监控		s			用户登录	登录
用户管理	-	u			用户注销	退出登录
2021-08-13 14:37:27		u		-	和規則設置	重调规则

行为规则配置

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以操作管理员账号登录操作日志页面,在左侧导航栏中单击操作日志,即可进入行为规则配置页面。

```
    说明
如忘记登录密码,可以提交工单找回密码。
```

 在行为规则配置页面,可以查看行为操作、行为分类、告警模板、备注、是否开启告警及相关操作,同时可按照行为分类、行为操作及危险等级,对行为规则 进行搜索。





行为规则配置

全部行为 🔻	全部操作 🔹 全部	等级 🔹			
行为操作	行为分类	告警模版	备注	危险等级	是否开启告警
登录	用户登录	有黑客入侵 ✔	1	低級 ▼	
修改密码	用户登录	1	1	低级 ▼	
退出登录	用户注销	1	1	低级 ▼	
系统资源监控重启	系统资源监控	1	1	低级 ▼	

字段说明:

○ 行为操作:用户对系统各个账户的功能操作。

○ 行为分类: 用户对系统功能操作所属的模块名

○ 告警模板: 用户执行操作时邮件所发送的告警内容

○ 备注:用户对行为规则的进一步说明。

○ 危险等级:对用户操作行为的评级,可设置行为危险等级,包括低级、中级及高级。

○ 是否开启告警:用户开启后,触发行为规则审计,则会发送告警信息,关闭后,只会记录操作,不会发送告警信息。

○ 操作:在告警模板操作栏,单击 ,即可对行为操作信息进行修改。
v5.0.8 系统管理 系统资源监控

🕥 腾讯云

最近更新时间: 2021-08-06 10:22:15

以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【系统资源监控】,即可进入资源监控页面,该页面包括系统详细信息、系统存储空间统 计和流量走势实时统计。

系统详细信息

系统详细信息包含系统产品名称、产品规格、当前版本等基础信息,以及数据安全审计总审计单元数参数信息。

系统详情	
产品名称	(二) 「重启」
产品规格	
当前版本	
连续运行时长	0年0月0天18小时17分31秒
系统当前时间	2021-04-21 14:42:26
购买峰值流量	3000 QPS
已用/总审计单元数	女2/3个
自定义规则数	1个

系统存储空间统计

存储空间统计用于展示数据安全审计实例当前的存储状态。在系统存储空间统计右上角,单击【清理剩余空间】,将清理的数据包含所选的日期。例如,选择了 12月1日至12月3日,则会删除12月1日、2日、3日,3天的数据。

()	说明
	统计报表将磁盘空间分为四个类型:

- 剩余空间:数据安全审计实例存储剩余空间;
- 系统占用空间: 数据安全审计自身代码所占存储空间;
- 审计日志占用空间:数据安全审计记录的数据库操作信息日志占用空间;
- 其他占用空间: 数据安全审计实例其他代码、配置文件占用空间。





流量走势实时统计

流量走势实时统计能统计一定时间跨度(最近 30 分钟、最近 24小时、最近 7 天)内数据安全审计中所审计的所有数据库的 QPS,确认全网 QPS 峰值是否超 过购买峰值,以帮助管理员了解数据安全审计性能状况,及时扩容升级产品。





用户管理

最近更新时间: 2025-05-27 16:30:32

以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中单击【用户管理】即可进入用户页面。

查看账号信息

账号管理用于管理 DSA 实例所有账号。系统管理员可以通过列表查看所有账号信息,包括所属角色、真实姓名、创建日期以及联系方式等。

🕛 说明

OTP 二维码:如需开启 OTP 实现登录双重验证,可在相应账号右侧操作栏,单击【OTP二维码】,或在数据安全审计管理页面右上角,找到管理员账 号下的 OTP 验证,单击【 OTP 验证】,查看原图并扫描动态校验码。

帐号名称	所雇角色	Y 真实姓名	创建日期	创建人	最后修改人	最后修改时间	联系方式	登录IP范围	操作
sysadmin	系统管理员		2020-09-28 10:00	系统默认创建	/	2020-10-20 16:52	电话: 邮稿: 微信:	评情	OTP二维码 编辑
useradmin	审计管理员		2020-09-28 10:00	系统默认创建	1	2020-09-28 10:00	电话: 邮稿: 微信:	详情	OTP二编码 编辑

添加账号

如需要增加管理员账号,单击【添加账号】,在弹框中填写账号信息,选择所属角色后,单击【确定】即可。

*账号:				
* 密码:				
* 真实姓名:				
* 手机号码:				
* 邮箱:				
* 微信号:				
* 所属角色:	审计管理员		V	
登录IP范围:	起始IP	结束IP	操作	
	0.0.0.1	255.255.255.255		
	添加 (当ip为ipv6格式时,仅对	"起始吧有效)		
			取消	确定

修改和删除账号

如需对账号进行修改或删除,可在相应账号操作列单击【编辑】或【删除】对账号进行调整。





帐号名称	所雇角色	▼ 真实姓名	创建日期	创现人	最后修改人	最后修改时间	联系方式	登录IP范围	操作
sysadmin	系统管理员		2020-09-28 10:00	系统默认创建	7	2020-10-20 16:52	电话: 邮箱: 概信:	汗病	OTP二维码 编辑
useradmin	审计管理员		2020-09-28 10:00	系统默认创建	7	2020-09-28 10:00	电话: 邮箱: 做信:	详惯	OTP二维码 编辑
sysaudit	操作审计管理员		2020-09-28 10:00	系统取认创建	7	2020-09-28 10:00	电话: 邮種: 做信:	详情	OTP二線码 编辑
-	审计管理员	-	2020-11-12 11:45	sysadmin	7	2020-11-12 11:45	电话: 1 邮箱:	详情	OTP三维码 网辑 問除



OTP 设置

最近更新时间: 2025-05-27 16:30:32

本文档将为您介绍如何开启 OTP 校验,并通过 OTP 校验登录数据安全审计管理页面。

操作步骤

÷

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【OTP 设置】,即可进入 OTP 设置页面。



3. 在 OTP 设置页面,设置校验开关,如需开启 OTP 验证选项,选中开启 OTP 验证,出现弹窗,根据提示扫 OTP 码,输入正确的 OTP 码,单击【确 定】,退出登录系统即可。

① 说明 建议开启 OTP 验证之前,提前	通知各管理员登录系统扫描OTP验证二维码,避免其无法登录该系统。	
OTP设置		

OTP设置	
	校验开关: ● 开启OTP验证 ○ 关闭OTP验证
	19 tr



4. 再次登录数据安全审计管理页面,需要输入OTP 校验码。





告警设置

最近更新时间: 2025-01-10 19:17:22

告警支持针对每个审计规则策略进行告警,告警支持邮件告警、syslog 告警,具体操作步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,在右侧操作栏,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【告警设置】,即可进入告警设置页面。

说明 如忘记登录密码,可以提交工单找回密码。

3. 在告警设置页面,分别对告警开关、系统资源告警配置、syslog 告警配置及邮件告警配置功能进行设置。

○ 告警开关

在告警设置页面,单击【告警开关】,分为【告警方式】和【告警内容】,打开需要开启告警的选项,单击【提交】,即可对 syslog 告警配置 中所设置 的服务器进行监控,且当满足告警条件时,将触发告警,并发送邮件至您所 配置的告警邮箱 中。

⚠ 注意 若需要接收告警信息,需打开邮件告警开关,且已在 邮件告警配置 中设置告警接收邮箱,否则无法接收告警信息。

古智井天	系统资源宣誓配置	syslog音音配置	即行合配直	
告警方式:	邮件告答: 17			syslog뜜쨜: 캐
告警内容:	QPS告答: 开			sql风脸告簪: 开 〇
	系統资源告答: 升 🔵			行为规则告答: 开 🔵
	agent掉线告警: <mark>开</mark>			
	提交			

○ 系统资源告警配置

在告警设置页面,单击【系统资源告警配置】,设置系统资源告警的触发条件,可将磁盘、内存、CPU 负载在0 - 100%之间调整,可自定义带宽值,单



击【提交】,即可对 syslog 告警配置 中所设置的服务器进行监控。



○ syslog 告警配置

⚠ 注意 目前 syslog 告警服务只支持 TCP 协议。

在告警设置页面,单击【syslog 告警配置】,输入需要记录的 syslog 服务器 IP 和端口,单击【提交】,即可完成 syslog 告警条件配置,设置完成 后将监控所配置的服务器。

系统资源告替配置	syslog告警配置	邮件告警配置
★ syslog服务器:		
* 诺口:		
	则试 提交	注: 目前syslog告誓服务只支持tcp

○ 邮件告警配置

单击【邮件告警配置】,依次填入邮件服务器的相关配置信息,如需添加多个收件人,请以英文分号分隔,填写完成后,单击【提交】,当满足告警条件 时,将发送邮件至所配置的邮箱中。





告警开关	系统资源告答配置 syslog告答配置 邮件告答配置
* SMTP服务器	: 第三方邮件服务容易受服务器反垃圾机制影响,如遇到不可用的,
二歳 *	建议尝试切换其他邮件服务:
* 邮件账号	:
* 密码	:
* 发件人	
收件人	字个收件人请以分号:分隔
SSL	: 🗸
	测试 提交 重置



时间服务器

最近更新时间: 2025-05-27 16:30:32

重置

时间服务器主要用于同步时间,找到您需要同步时间的服务器IP进行设置即可,具体操作步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,在右侧操作栏,单击【管理】,进入数据安全审计登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 使用 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【时间服务器】,即可进入时间服务器设置页面。

	 说明 如忘记登录密码,可以提交工单找回密码。 	
3.	在时间服务器设置页面,输入 NTP 服务器 IP,单击【提交】,即可完成设置。	
	时间服务器设置	
	* NTP服务器IP: 请输入NTP服务器IP	

4. 设置完成后,数据安全审计系统时间会与您设置的 NTP 服务



备份服务器设置

最近更新时间: 2025-05-27 16:30:32

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【备份服务器设置】,即可进入备份服务器设置页面。

如忘记登录密码,可以 提交工单 找回密码。

在备份服务器设置页面,依次输入备份服务器地址、备份服务器端口、备份服务器用户名、备份服务器密码、备份服务器目录路径,打开备份开关,单击【保存】即可完成备份服务器设置。

说明

- 备份服务器地址需为公网 IP 地址,并且入站安全组是放通状态,详情请参见 添加安全组规则 。
- 备份服务器通过 SSH 的方式进行备份,备份服务器设置成功后,系统每日02:00(UTC+8)定时备份前一天的数据到目标机器目录。

备份服务器设置	
备份服务器地址:	
备份服务器端口:	22
备份服务器用户名:	root
备份服务器密码:	
备份服务器目录路径	/data/beifen
备份开关:	Я
[保存

- 4. 设置完成后,数据安全审计管理系统中的数据将会按照设置路径进行备份。
- 5. (可选)如需恢复之前存在的数据,在备份服务器设置页面,单击【数据恢复】页签。
- 6. (可选)在数据恢复页签中,单击【数据恢复】,选择恢复日期并导入恢复数据即可。

数据恢复				Х	
恢复日期:	请选择日期	Ë	备份文件:	土 点击上传文件	
				关闭	

审计管理 安全审计与分析 审计数据

最近更新时间: 2025-05-27 16:30:32

审计概览

- 1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面,详情可参见 控制台登录。
- 2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择**安全审计与分析 > 审计概览**,即可进入审计概览页面。
- 在审计概览页面中,可总览全网数据库日志信息,态势分析,风险占比以及查询单个数据库资产详细信息,如需了解数据库资产审计详细内容,可在审计概览 页面下方查询详细信息。
 - **日志总数**:用于统计全网各数据资产日志总数。
 - 今日日志:用于统计全网各数据资产今日日志总数。
 - 今日风险:用于统计全网各数据资产今日风险总数。
 - **今日会话:**用于统计全网各数据资产今日会话总数。
 - 态势分析:可查看您所配置的审计单元的审计趋势,风险趋势,会话趋势,还可按照高风险、中风险、低风险进行查看各个风险级别详细数据,每个报表 可展示三种走势图及三类风险级别数据:
 - **审计趋势**:用于展示数据资产的审计单元语句压力,展示时间有24小时、7天、30天。
 - 风险趋势:用于展示数据资产的审计单元高中低三类风险的统计信息,展示时间有24小时、7天、30天。
 - 会话趋势:用于展示数据资产的审计单元各类会话信息,展示时间有24小时、7天、30天。
 - 风险占比统计:用于显示数据资产对应的命中风险等级。
 - 风险等级:用于展示数据资产审计单元有关的自定义规则命中风险信息,展示时间有24小时、7天、30天。
 - 数据资产:用于展示被命中的数据资产,展示时间有24小时、7天、30天。
 - 资产审计:主要展示单个数据资产的会话总数,DDL 操作数量、失败会话数量、最大并发会话及风险数等信息。

日本色数 30.38万余 巴尼行 0루 3天 32 가리 엔터넷用: 新紀島 18.568 / 5068 新兵島 1.9768 / 19768	◆日日本 8.34万余 日刊社: 74%▲ 用刊社: 183	今日风险 0↑ 日环比:0%▼		周环比: 0%▼	今日会谱 1.15 万次 日环北:92%▲	MEIFEL: 680%▲
24小时 24小时	7天 30天 2021-03-10 ~ 2021-03-16 □	风险占比统计		24小时	7天 30天 2021-03-10	~ 2021-03-16
		1004 0-30	£8 752		570,070 570,070 600,000 600,00	

日志检索

日志检索主要提供日志查询与导出功能。

- 1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面,详情可参见控制台登录。
- 2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择**安全审计与分析 > 审计日志**,即可进入审计日志页面。
- 管理员通过 审计概览 定位到疑似有风险的数据库审计单元,或者企业网络已经发生数据库安全问题时,可在日志检索页面查询并导出日志信息。

救強	<u>約</u> 严東型:	全部	✓	8 V						
7424	₽ ¹ R: <u></u>		∨ 用户名	: IMAA		# ## ##		1	<u>五</u> 岡 母出 展开∨	
10	<u>ifi</u> —d \8 f 4	天静天本闻上闻	本月 上月 目症义							
() <u>s</u> iser	£,数据总量:22,267 条								
序	e	数据库用户	查户跳IP	时间	命中規則	10(17)	审计单元省	风险等级	SQLI最份	
1				04-20 16:55:05				 中风险 		
2				04-20 16:56:10				• 正常		

日志查询

在日志检索页面,您可以按照审计单元、风险等级、用户名、命中规则及时间,对日志进行查询。



数据资产类型: 全部 ∨	数据资产: 全部 ∨		
风险等级: 全部	✓ 用户名: 请输入	命中规则: 请选择 >>	●出 展开∨
<u>銀近一小时</u> 今天 昨天 本周 上周 本月 上月	目定义		

查看数据详情

在日志列表中,可单击某条记录查看其详细内容。

操作语句:	
操作类型:	INSERT
操作时间: SessionID:	01-06 17:25:03
命中规则:	insert
风险等级:	◎ 低风险
数据库: 数据库ID·	
数据库用户:	
表名:	
影响行数:	1
执行时间:	0 ms
返回消息:	
返回码:	0
审计组ID:	
客户端IP:	
访问源业务部门:	
包长度:	
使用工具:	
终端名称:	

日志导出

检索出需要导出的数据,现已支持不限数量导出,在列表上方单击**导出**,弹出导出数据弹窗,单击确定即可将数据导出,导出文件类型为 Excel(.xlsx格式)。

Excel文件生成	×
导出记录16,075,835条,确认要导出吗? 注:尽量缩小范围导出,导出数量过多,会影响服务性能	
取消	确定



规则配置

最近更新时间: 2025-05-27 16:30:32

规则配置页面可配置触发风险告警的命中规则。数据安全审计已提供17个内置规则,可满足大多数安全场景,内置规则不可删除、不可编辑。您也可以根据业务 需要,添加自定义规则,下面将为您详细介绍配置操作。

操作步骤

以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中,选择【安全审计与分析】>【规则配置】即可进入规则配置页面。

新建规则

如需自定义规则满足个性化审计需求,单击【添加规则】,进入新建规则页面,填写规则名称等,单击【保存】即可。

△ 注意

- 规则配置支持同一规则配置多个条件,多个条件之间为 "与" 关系,必须全部匹配才能够触发规则和告警。
- 自定义规则默认为黑名单,触发后将产生告警并且记录入库。如果管理员需要节省数据安全审计的审计单元的存储空间,指定部分操作行为不记录不 入库,可在规则中指定相关操作后,选择"白名单"选项,并且将告警选项都取消。

以上操作完成后,即可实现白名单类型规则配置,减少误报、减轻数据安全审计的审计单元存储压力。

• 规则示例

在规则配置页面,单击【添加规则】,按下图配置规则,表名和阈值根据您的业务场景自行设定,单击【保存】即可。



添加规则				
基础信息				
规则类型	● 黑名单 (
* 规则名称	请输入规则	名称		
规则备注	请输入规则	备注		
风险等级	 ● 低风险 (🔵 中风脸 🔵 高	网络	
规则定义				
客户端	客户端IP	包含 >	可配置多个IP, 英文逗号分隔, 如: 192.168.1.1,19	添加
服务端	数据库IP	包含 🗸 🗸	可配置多个IP, 英文逗号分隔, 如: 192.168.1.1,19	添加
	数据库端□	大于等于 🗸 🗸	请输入数据库端口,范围1-65535	添加
	致掘库用户	包含 🗸	可配置多个用户,英文逗号分隔,如:sys,root,sys	添加
	数据库名	包含 🗸	可配置多个数据库名,英文逗号分隔,如:mysql.t	添加
行为	操作类型	包含 🗸 🗸	select	添加
	操作语句	包含 🗸		添加
	表名	包含 🗸 🗸	xx_test	添加
语句执行	执行时长	大于等于───	请输入数值,取值范围0-9999	添加
	影响行数	大于等于 ∨	50 行	添加
时间限制	操作时间	大于等于 🗸 🗸	请选择日期	添加

• 规则配置建议

以下三个建议规则仅作为示例,用户可根据自身业务自行配置。



○ 防爬取规则:防止使用例如 select 操作语句,爬取表数据。

添加规则					2
基础信息					
规则关型	◉ 黑名单	白名单			
* 规则名称	请输入规则	名称			
规则备注	请输入规则	备注			
风险等级	● 低风险	○ 中风险 ○	高风	脸	
规则定义					
客户端	客户端IP	包含	\vee	可配置多个IP, 英文逗号分隔, 如: 192.168.1.1,19	添加
服务端	数据库IP	包含	\sim	可配置多个IP, 英文逗号分隔, 如: 192.168.1.1,19	添加
	数据库端口	大于等于	\vee	请输入数据库端口,范围1-65535	添加
	数据库用户	包含	\sim	可配置多个用户,英文逗号分隔,如:sys.root.sys	添加
	数据库名	包含	\vee	可配置多个数据库名,英文逗号分隔,如:mysql.t	添加
行为	操作类型	包含	\vee	select	添加
	操作语句	包含	\sim		添加
	表名	包含	\sim	请输入表名,多个用英文逗号隔开	添加
语句执行	执行时长	大于等于	\sim	请输入数值,取值范围0-9999	添加
	影响行数	大于等于	\vee	100 行	添加
时间限制	操作时间	大于等于	\vee	请选择日期	添加

▲ 注意

影响行数可以根据业务自行配置。



○ 慢查询发现规则:检查执行时间较长的 SQL 语句,便于进行优化。

비급문					
规则类型	● 黑名单 (白名单			
规则名称	请输入规则	各称			
规则备注	请输入规则	昏注			
风险等级	● 低风险 () 中风险		· 建金	
则定义					
客户端	客户端IP	包含	\vee	可配置多个IP, 英文逗号分隔, 如: 192.168.1.1,19	添加
服务端	数据库IP	包含	\sim	可配置多个IP,英文逗号分隔,如:192.168.1.1,19	添加
	数据库端口	大于等于	\sim	请输入数据库端口,范围1-65535	添加
	数据库用户	包含	~	可配置多个用户,英文逗号分隔,如:sys,root,sys	添加
	数据库名	包含	\sim	可配置多个数据库名,英文逗号分隔,如:mysql.t	添加
行为	操作类型	包含	\sim	select	添加
	操作语句	包含	\sim		添加
	表名	包含	\sim	请输入表名,多个用英文逗号隔开	添加
语句执行	执行时长	大于等于	\sim	500 室秒	添加
	影响行数	大于等于	\sim	请输入数值,取值范围0-9999	添加
时间限制	操作时间	大于等于	\sim	请选择日期	添加

执行时间可以根据业务自行配置。

○ 危险操作规则:检查执行 DELETE/DROP/ALTER 等类型的高危 SQL 语句。

信息					
则类型	 黑名单) 白名单			
规则名称	请输入规则	名称			
规则备注	请输入规则	备注			
风险等级	● 低风险	○ 中风险		U2	
则定义					
客户端	客户端IP	包含	V	可配置多个IP,英文逗号分隔,如:192.168.1.1,19	添加
服务端	数据库IP	包含	\sim	可配置多个IP, 英文逗号分隔, 如: 192.168.1.1,19	添加
	数据库端口	大于等于	\sim	请输入数据库端口,范围1-65535	添加
	数据库用户	包含	\sim	可配置多个用户,英文逗号分隔,如:sys.root.sys	添加
	数据库名	包含	\sim	可配置多个数据库名,英文逗号分隔,如:mysql.t	添加
行为	操作类型	包含	\sim	drop	添加
	操作语句	包含	\vee		添加
	表名	包含	\sim	请输入表名,多个用英文逗号隔开	添加
语句执行	执行时长	大于等于	\sim	请输入数值,取值范围0-9999	添加
	影响行数	大于等于	\sim	请输入数值,取值范围0-9999	添加

修改规则

🔗 腾讯云

在规则列表中,找到需要修改的规则,在右侧操作栏中,单击【编辑】,修改信息后单击【保存】即可。

规则列表 规则应用						
+ X5.008391 () 80% (M77	現時配置					
规则名称	规则类型	规则属性	风险等级	关联数据资产	备注	操作
AIÐIS	白名单	内置规则		全部	系统内置规则	编辑
 CVE引奉 	白谷单	内置规则		全部	系统内置规则	明祖
3956783	黑名单	目虛义規則	市市			编辑 新种

删除规则

在规则列表中,找到需要删除的规则,在右侧操作栏中,单击【删除】,再单击询问窗【确定】即可。

現到列表 現到雇用						
/ 规则名称	规则换型	规则描述	风险等级	关联数据资产	音注	援作
AI引擎	白名单	内置规则		全部	系統內置規則	605 <u>8</u>
CVE3IP	白谷单	内置规则		全部	系统内置规则	 28時以要服除均7 取 消 報 注
I RECERT	扁谷单	自意义规则	憲政			5048 1939



审计报表

最近更新时间: 2025-05-27 16:30:32

审计报表功能主要展示所有配置过的审计组数据,并提供搜索、查看及 PDF 下载功能,具体操作步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【安全审计与分析】>【审计报表】,即可进入审计报表页面。

说明 如忘记登录密码,可以提交工单找回密码。

3. 在审计报表页面中,可查看内容包括报告名称、报告说明及发送目标等字段,同时可以进行相关操作,每个页面默认展示10条数据,可按照报告名称、生成方 式、开始时间及结束时间,对报告进行搜索,还可下载 PDF 报告。

新建报表						
报告名称:	生成方式: 全部 🗸	时间: 开始日期	~ 结束日期 首	搜索		
报表名称	报表说明	发送目标	报表生成时间	报表类型	状态	操作
审计日报_2021-03-15	日报		2021-03-15 21:00:02	定时生成	◎ 已生成	查看 pdf下载 删除
报告_2021-03-14	1		2021-03-14 17:00:01	定时生成	◎ 已生成	查看 pdf下载 删除
报告_2021-03-13	1		2021-03-13 17:00:02	喧时生成	◎ 已生成	查看 pdf下载 删除

• 定时生成报表

数据安全审计管理系统支持定时生成报表。

在报表上方单击【新建报表】,弹出新建报表弹窗,选择"定时报表",并依次输入模板名称、统计周期(可选择定时执行、每天一次、每周一次、每月一次)、执行时间(精确到时分秒)、报告说明,设置完成后,单击【确定】,即可在您设定的执行时间定时生成报表。

新建报表		\times
报告类型:	🔾 即时报表 🧿 定时报表	
* 模板名称:	审计日报 最多30个字符	
统计周期:	每天一次 🗸	
* 执行时间:	21:00:00 ① 注:建议导出时间为凌 晨1点	
* 报告说明:	日报	
	最多200个字符	
	取消 确	定

• 即时生成报表

数据安全审计管理系统支持即时生成报表,即生成某个时间段内的报表。

在报表上方单击【新建报表】,弹出新建报表弹窗,选择"即时报表",依次输入报告名称、审计单元、统计开始时间、统计结束时间、报告说明,单击【确 定】,即可输出您规定的时间范围内的报表。

⚠ 注意 开始时间应早于结束时间。



新建报表		×
报告类型:	● 即时报表 ○ 定时报表	
* 报告名称:	最多30个字符	
审计单元:		V
* 统计开始时间:	2021-03-15 00:00:00	
* 统计结束时间:	2021-03-15 23:59:59	Ë
* 报告说明:	最多200个字符	10
		取消 确定



数据资产与 Agent

最近更新时间: 2025-05-27 16:30:32

Agent 下载

- 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,即可进入审计用 Agent 页面。
- Agent 部署。在审计用 Agent 页面,选择Agent 下载 > 添加 Agent,可配置审计 Agent 的各类参数并提供下载链接,配置步骤以及配置注意事项,请参见 Agent 部署。
- 3. 添加完成 Agent 后,在 Agent 配置页面,可查看所有已正确安装且能实现 DSA (Data Security Audit)实例网络互通的 Agent 信息。

Agent下载	Agent列表				
添加Agent					
Agent 名称		审计服务 IP	审计服务通口	数据资产	提作
					下號 🗸 🛛 🗍 🕅 除

列表各字段含义如下:

- Agent 名称:用于配置该 Agent 的名称。
- 审计服务 IP: Agent 回传数据的源 IP。
- 审计服务端口: 该 Agent 配置的审计端口。
- 数据库资产:可查看该 Agent 审计的数据库的所有 IP 地址。
- 操作:用于下载该 Agent 的链接。
 - 在右侧操作栏,选择下载 > 下载 Linux Agent或下载 Windows Agent,弹出部署 IP 窗口,单击确定即可开始下载 Agent。

△ 注意

- 若部署机器操作系统 CentOS 版本号小于7 或者 Ubuntu 版本号小于11,必须勾选下方说明,否则无法部署 Agent。
- 请添加安装包需要部署机器的 IP 或 IP 列表。
- 如未添加 IP 信息却部署了会导致 Agent 无法启动。
- 如有新的机器要部署请重新下载安装包并填写机器的 IP 信息。

山見IF /	C
部署机器操作系统centos版本号小于7 或者ubuntu 版本号小于11 (注:若 部署机器操作系统centos版本号小于7 或者ubuntu 版本号小于11,必须勾选此选项,否则 无法部署agent)	J
取消 确定	

○ 在右侧操作栏,选择**下载 > Linux 批量部署**,输入部署地址,支持按 IP 或按 IP 段部署,支持添加多行,输入服务器 IP 、SSH 端口号、用户 名、密码,输入完成后单击确定即可。



linux批量部署							×
部署地址: 部署机器 ubuntu版本号 按IP部署 按	/data/dbAudit/ 操作系统centos版 小于11,必须勾选此道 IP段部署	本号小于7 或者ub ^{起页,} 否则无法部署a	untu 版本号小 gent)	于11 (注: 耤	昭晋机器操作系统	centos版本号小于i	7 或者
服务器IP		SSH端口号 22	用户 ro	名 ot	密码	ø	操作
<mark>添加一行</mark> 注: ①SSH的 帐号 ②SSH端口号	密码服务器不会保存5 默认22、用户名默认r	R做下发服务使用 bot,可自行修改					
						取消	确定

○ 在右侧操作栏,单击删除,可删除该条 Agent 信息。

Agent 列表

- 1. 以 useradmin 账号登录数据安全审计管理页面,在左侧导航栏中,选择审计用 Agent > Agent 列表,即可进入审计列表中。
- 2. 在审计列表中,可以查看所有已配置的 Agent。Agent 列表默认展示内容包括:Agent 名称、部署 Mac、部署 IP、操作系统、部署时间、最新上报时间、 运行状态、开启状态及相关操作。
 - 搜索: 您可以按数据资产、Agent 状态、Agent名称、IP、对 Agent 进行搜索。
 - 查看 Agent 配置详情:在"操作"栏中,单击编辑,可以查看 Agent 配置相关信息。
 - 相关操作:在右侧操作栏,可以对 Agent 进行启动、停止、编辑、卸载、删除的相关操作。

Agent下號 Agent判罚									
数据资产: 全部	✓ Agentită: ±B ∨						Agent各称 V 地入	agent 笞称//IP	Q,
Agent 名称	部署 Mac	CI椰 IP	操作系统	25400)/A	最新上版时间	运行状态	开盘状态	爆作	
			linux	2021-04-19 21:14:00	2021-04-20 17:22:42	◎ 進行中		1997 - 20 1 0 - 1992	
								共1条,当前显示1-1条 <	1 >





最近更新时间: 2025-01-10 19:17:22

审计单元配置可为从属于一个应用的一台或多台数据库服务器进行命名,方便后续规则配置或审计信息时,使用直观的名字来表达数据库信息,优化策略和报表可 读性。下面将为您详细介绍配置操作。

- 2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择**配置管理 > 审计单元**,即可进入审计单元配置页面。

	① 说明 若审计 Agent 部署	成功,会默认添加审计单元,无需自己新建。	
3.	在审计单元列表中,找到需	要修改的审计单元(建议以业务应用名称为基础命名),在右侧操作栏单击 编辑 ,在弹框中修	没信息后,单击 确定 即可。
	修改审计单元		Х
	* 审计单元名称: * 数据资产实例: 业务名: * 备注信息:	× 如未找到相应业务,可点击这 里 添加 添加资产时自动添加的	
		取消 确	定



访问源配置

最近更新时间: 2021-11-24 10:28:35

访问源配置可为从属于同一部门或同一网络区域的访问 IP 段进行命名,方便后续规则配置、审计信息使用直观名字来表达数据库访问端信息,优化策略以及报表 可读性。下面将为您详细介绍配置操作。

以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择**配置管理 > 访问源**,即可进入访问源配置列表页面。

• 添加访问源

单击列表上方添加,在弹出窗口中,填写业务名、访问源名称、访问源包含 IP 段、备注信息,单击确定即可。

添加访问源			
• <u>业</u> 务名:			
	如未找到相应业务,可点;	击这里添加	
•访问源名称:	请输入访问源名称		
访问源包含IP段:	起始IP	结束IP	操作
	0.0.0.1	255.255.255.254	
	増加		
• 备注信息:	请输入备注信息		
			取消 确意

• 修改访问源

在访问源列表中,找到需要修改的访问源,在右侧操作栏中,单击**修改**,在弹框中修改信息后,单击**确定**即可。

1X10119118			,
• <u>业</u> 务名:			
	如未找到相应业务,可点	击这里添加	
•访问源名称:			
访问源包含IP段	起始IP	结束IP	操作
	127.0.0.1	127.255.255.254	
	增加		
* 备注信息:	ds		
			取 淌 确 定

• 删除访问源

在访问源列表中,找到需要删除的访问源,在右侧操作栏中,单击**删除**,再单击询问窗中的确定即可。

访问源名称	包含IP段数量	部门及业务名	备注	 您确认要删除吗?
	1		ds	取消 确定
	1		ds	修改 删除



部门业务配置

最近更新时间: 2025-01-10 19:17:22

部门业务配置功能主要是部门配置与业务配置的相关功能,具体配置步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中,选择**配置管理>部门&业务**,即可进入部门业务配置页面。

•	说明				
	如忘记登录密码,	可以	提交工单	找回密码。	

- 3. 在部门业务配置页面,可进行部门配置及业务配置。
- 部门配置
 - 3.1 在部门业务配置页面,单击**部门配置**,可添加并查看部门名、部门负责人及备注,同时可进行相关操作。

部门配置业务配置			
+ 添加部门 合删除			
部门名	部门负责人	备注	操作
test	小李		修改 删除
it运营部	马忠义		修改 删除
财务部	王五		修改 删除
□ 采购部	赵四		修改 删除

3.2 在部门设置页面,单击**添加部门**,在弹出的添加部门窗口中,填写部门名、部门负责人以及备注信息,单击确定即可完成添加。

添加部门	×
	1214 \ 107747
· Dr. Ma •	宿園八即 J名
*部门负责人:	请输入部门负责人
备注信息:	请输入备注信息
	取消 确定

3.3 添加完成后,已添加的部门将出现在部门配置列表中,支持对已添加的部门进行修改或删除,且支持对部门信息批量选择删除。

部门曹	記置 业务配置			
+ 添	加部门 ① 删除			
	部门名	部门负责人	备注	操作
	test	小李		修改 删除
	it运营部	马忠义		修改 删除



○ 修改

找到需要修改的部门信息,在右侧操作栏单击**修改**,在弹出框中可以修改对应部门信息。

- 删除
- 方式1: 找到需要删除的部门信息,在右侧操作栏单击删除,在弹出框中确认删除,即可完成删除。
- **方式2**:选择需要删除的部门,在列表上方单击**删除**,即可批量删除部门信息。

• 业务配置

3.1 在部门业务配置页面,单击**业务配置**,可添加并查看业务名、业务负责人、部门名及备注,同时可进行相关操作。

部门曹	部门配置 业务配置										
+ 添加业务											
	业务名	业务负责 人	部门名	备注	操作						
	test	小赵	test		修改 删除						
	薪资结算系统	meller	财务部	18	修改 删除						

3.2 在业务配置页面,单击**添加业务**,在弹出的添加业务窗口中,填写部门名、业务名、业务负责人以及备注信息,填写完成后,单击**确定**即可完成添加。

添加业务		×
*部门名:		\vee
* <u>业</u> 务名:	请输入业务名	
* 业务负责人:	请输入业务负责人	
备注信息:	请输入备注信息	
		取消 确定

3.3 添加完成后,已添加的业务将出现在业务配置列表中,支持对已添加的业务进行修改或删除,且支持对业务信息进行批量选择删除。

部门	部门配置 业务配置									
+ ž	+ 添加业务									
	业务名	业务负责 人	部门名	备注	操作					
	test	小赵	test		修改 删除					
	薪资结算系统	meller	财务部	18	修改 删除					

○ 修改

找到需要修改的业务信息,在右侧操作栏单击**修改**,在弹出框中可以修改对应业务信息。

○ 删除

- 方式1: 找到需要删除的业务信息,在右侧操作栏单击**删除**,在弹出框中确认删除,即可完成删除。
- **方式2**:选择需要删除的业务,在列表上方单击**删除**,在弹出框中确认删除,即可批量删除业务信息。



操作日志管理

最近更新时间: 2025-01-10 19:17:22

操作审计员负责审计数据安全审计各管理员的操作,防止其他管理员滥用职权进行非法操作。用操作管理员账号登录后,能够阅览管理员操作日志列表并对行为规 则进行配置。

日志检索

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以操作管理员账号登录操作日志页面,在左侧导航栏中单击**行为规则配置**,即可进入操作日志页面。

① 说明 如忘记登录密码,可以 提交工单 找回密码。

3. 在操作日志页面,您可以根据操作事件、操作 IP、行为分类、操作时间检索还原非法操作完整信息。

操作日志							
操作帐户:	操作IP:	行为分类:	全部へ	操作时间:	开始日期 ~ 结束日期 前	搜索	
			全部	•			
操作时间	操作账	ب	退出		操作IP	行为分类	操作行为
2018-05-25 11:28:36	userad	min	新増配置修改配置		14.17.22.33	检索日志	检索日志
2018-05-25 11:28:35	userad	min	删除配置		14.17.22.33	检索日志	日志检索
2018-05-25 11:28:34	userad	min	12.8100	•	14.17.22.33	检索日志	日志检索

行为规则配置

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

购买时	间	到期时间	操作
2020-4	-14	2020-5-14	管理 续费 升级

2. 以操作管理员账号登录操作日志页面,在左侧导航栏中单击**行为规则配置**,即可进入行为规则配置页面。



 在行为规则配置页面,可以查看行为操作、行为分类、告警模板、备注、是否开启告警及相关操作,同时可按照行为分类、行为操作及危险等级,对行为规则 进行搜索。





行为	分类: 全部	∨ 行为操作:	全部 🗸	危险等级 : 全部	∨ 搜索		
	行为操作	行为分类	告警模版	备注	危险等级	是否开启告警	操作
	登쿴	用户登录	报告,有敌人来了,.		低级>	开启	修改
	修改密码	用户登录			低级~	()关闭	修改

字段说明:

- 行为操作:用户对系统各个账户的功能操作。
- 行为分类:用户对系统功能操作所属的模块名
- 告警模板: 用户执行操作时邮件所发送的告警内容
- 备注:用户对行为规则的进一步说明。
- 危险等级:对用户操作行为的评级,可设置行为危险等级,包括低级、中级及高级。
- 是否开启告警:用户开启后,触发行为规则审计,则会发送告警信息,关闭后,只会记录操作,不会发送告警信息。
- ○操作:在目标行为右侧操作栏,单击修改,即可对行为操作信息进行修改。

修改配置		×
行为操作:	登录	
行为分类:	用户登录	
接口路由:		
告警信息模板:	报告,有敌人来了,请注意,小心敌方陷阱	
备注:		
危险等级:	低级	\sim
是否开启告答:	● 关闭	
	取消	确定

v5.0.7 系统管理 系统资源监控

🕥 腾讯云

最近更新时间: 2021-08-06 10:23:47

以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【系统资源监控】,即可进入资源监控页面,该页面包括系统详细信息、系统存储空间统 计和流量走势实时统计。

系统详细信息

系统详细信息包含系统产品名称、产品规格、当前版本等基础信息,以及数据安全审计总审计单元数参数信息。

系统详情	
产品名称	重启
产品规格	
当前版本	
连续运行时长	0年0月0天18小时17分31秒
系统当前时间	2021-04-21 14:42:26
购买峰值流量	3000 QPS
已用/总审计单元数	女2/3个
自定义规则数	1个

系统存储空间统计

存储空间统计用于展示数据安全审计实例当前的存储状态。在系统存储空间统计右上角,单击【清理剩余空间】,将清理的数据包含所选的日期。例如,选择了 12月1日至12月3日,则会删除12月1日、2日、3日,3天的数据。

()	说明
	统计报表将磁盘空间分为四个类型:

- 剩余空间:数据安全审计实例存储剩余空间;
- 系统占用空间: 数据安全审计自身代码所占存储空间;
- 审计日志占用空间:数据安全审计记录的数据库操作信息日志占用空间;
- 其他占用空间: 数据安全审计实例其他代码、配置文件占用空间。





流量走势实时统计

流量走势实时统计能统计一定时间跨度(最近 30 分钟、最近 24小时、最近 7 天)内数据安全审计中所审计的所有数据库的 QPS,确认全网 QPS 峰值是否超 过购买峰值,以帮助管理员了解数据安全审计性能状况,及时扩容升级产品。





用户管理

最近更新时间: 2025-05-27 16:30:32

以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中单击【用户管理】即可进入用户页面。

查看账号信息

账号管理用于管理 DSA 实例所有账号。系统管理员可以通过列表查看所有账号信息,包括所属角色、真实姓名、创建日期以及联系方式等。

🕛 说明

OTP 二维码:如需开启 OTP 实现登录双重验证,可在相应账号右侧操作栏,单击【OTP二维码】,或在数据安全审计管理页面右上角,找到管理员账 号下的 OTP 验证,单击【 OTP 验证】,查看原图并扫描动态校验码。

帐号名称	所屬角色	T 真实姓名	创建日期	创建人	最后修改人	最后修改时间	联系方式	登录IP范围	操作
sysadmin	系统管理员		2020-09-28 10:00	系统默认创建	7	2020-10-20 16:52	电话: 邮稿: 微信:	评慎	OTP二维码 编辑
useradmin	审计管理员		2020-09-28 10:00	系统默认创建	7	2020-09-28 10:00	电话: 邮稿: 微信:	详情	OTP二维码 编辑

添加账号

如需要增加管理员账号,单击【添加账号】,在弹框中填写账号信息,选择所属角色后,单击【确定】即可。

*账号:				
*密码:				
* 真实姓名:				
* 手机号码:				
* 邮箱:				
★微信号:				
* 所属角色:	审计管理员		v	
登录IP范围:	起始IP	结束IP	操作	
	0.0.0.1	255.255.255.255		
	添加 (当ip为ipv6格式时,仅对	超始19有效)		
			取消	确定

修改和删除账号

如需对账号进行修改或删除,可在相应账号操作列单击【编辑】或【删除】对账号进行调整。





账号名称	所屬角色	7 真实姓名	创建日期	创建人	最后修改人	最后修改时间	联系方式	登录IP范围	操作
sysədmin	系统管理员		2020-09-28 10:00	系统默认创建	7	2020-10-20 16:52	电话: 邮稿: 御信:	汗病	OTP二维码 编辑
useradmin	审计管理员		2020-09-28 10:00	系统默认创建	7	2020-09-28 10:00	电话: 邮箱: 你信:	详惯	OTP二维码 编辑
sysaudit	操作审计管理员		2020-09-28 10:00	系统默认创建	7	2020-09-28 10:00	电话: 邮箱: 你伯:	详情	OTP二编码 编辑
-	审计管理员		2020-11-12 11:45	sysadmin	7	2020-11-12 11:45	电话: 1 邮箱: 微信:	详情	OTP三维码 编辑 删除



OTP 设置

最近更新时间: 2025-05-27 16:30:32

本文档将为您介绍如何开启 OTP 校验,并通过 OTP 校验登录数据安全审计管理页面。

操作步骤

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【OTP 设置】,即可进入 OTP 设置页面。



3. 在 OTP 设置页面,设置校验开关,如需开启 OTP 验证选项,选中开启 OTP 验证,出现弹窗,根据提示扫 OTP 码,输入正确的 OTP 码,单击【确 定】,退出登录系统即可。

() 说明		
建议开启 OTP 验证之前,	提前通知各管理员登录系统扫描OTP验证二维码,	避免其无法登录该系统。

OTP设置		
	校验开关: ● 开启OTP验证 ○ 关闭OTP验证	
	保存	

4. 再次登录数据安全审计管理页面,需要输入OTP 校验码。

数据安全审计
A 请输入您的用户名
8 请输入您的密码
贸 请输入您的otp校验码
登录
本系統已支持IPV6,講使用chrome浏览器,点击下载!



告警设置

最近更新时间: 2025-01-10 19:17:22

告警支持针对每个审计规则策略进行告警,告警支持邮件告警、syslog 告警,具体操作步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,在右侧操作栏,单击管理,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击告警设置,即可进入告警设置页面。

说明 如忘记登录密码,可以提交工单找回密码。

QPS告答: 开〇

3. 在告警设置页面,分别对告警开关、系统资源告警配置、syslog 告警配置及邮件告警配置功能进行设置。

○ 告警开关

在告警设置页面,单击**告警开关**,分为**告警方式**和**告警内容**,打开需要开启告警的选项,单击**提交**,即可对 syslog 告警配置 中所设置的服务器进行监 控,且当满足告警条件时,将触发告警,并发送邮件至您所 配置的告警邮箱 中。

注意 若需要接收告警信息,需打开邮件告警开关,且已在 邮件告警配置 中设置告警接收邮箱,否则无法接收告警信息。 告警开关 系统资源告警配置 syslog告警配置 邮件告警配置 音響方式: 邮件告答: ① 图件告答: ① 图件告答: ① 图件告答: ① ①

系統資源告答: 17 🔵	行为规则告警: 开 🔵
agent掉线告答: <mark>开</mark> 🔵	
縱交	
艾休汝在什教工里	

○ 系统资源告警配置

告警内容:

在告警设置页面,单击**系统资源告警配置**,设置系统资源告警的触发条件,可将磁盘、内存、CPU 负载在0 - 100%之间调整,可自定义带宽值,单击提

sql风险告警: 开〇



交,即可对 syslog 告警配置 中所设置的服务器进行监控。



○ syslog 告警配置

⚠ 注意 目前 syslog 告警服务只支持 TCP 协议。

在告警设置页面,单击**syslog 告警配置**,输入需要记录的 syslog 服务器 IP 和端口,单击**提交**,即可完成 syslog 告警条件配置,设置完成后将监控 所配置的服务器。

系统资源告替配置	syslog告警配置	邮件告警配置
* syslog服务器:		
* 端口:		
	测试 提交	注: 目前syslog告警服务只支持tcp

○ 邮件告警配置

单击**邮件告警配置**,依次填入邮件服务器的相关配置信息,如需添加多个收件人,请以英文分号分隔,填写完成后,单击**提交**,当满足告警条件时,将发 送邮件至所配置的邮箱中。

▲ 注意

若填写 QQ 邮箱账号,密码需填写所设置的邮箱密码。



告警开关	系统资源告答配置 syslog告答配置 邮件告答配置
* SMTP服务器	
* 端口	第三方邮件服务容易受服务器反垃圾机制影响,如遇到不可用的, 建议尝试切换其他邮件服务 :
* 邮件账号	:
* 密码	
* 发件人	
收件人	2 多个收件人请以分号: 分隔
SSL	: 🔽
	测试 提交 重苦


时间服务器

最近更新时间: 2025-05-27 16:30:32

时间服务器主要用于同步时间,找到您需要同步时间的服务器IP进行设置即可,具体操作步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,在右侧操作栏,单击管理,进入数据安全审计登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 使用 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击时间服务器,即可进入时间服务器设置页面。

()	说明				
	如忘记登录密码,	可以	提交工单	找回密码。	

3. 在时间服务器设置页面,输入 NTP 服务器 IP,单击提交,即可完成设置。

时间服务器设置	
* NTP服务器IP:	请输入NTP服务器IP
提交重	苦

4. 设置完成后,数据安全审计系统时间会与您设置的 NTP 服务器地址所在时间进行同步。



备份服务器设置

最近更新时间: 2025-05-27 16:30:32

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【备份服务器设置】,即可进入备份服务器设置页面。

 说明 如忘记登录密码,可以提交工单找回密码。 	
---	--

在备份服务器设置页面,依次输入备份服务器地址、备份服务器端口、备份服务器用户名、备份服务器密码、备份服务器目录路径,打开备份开关,单击【保存】即可完成备份服务器设置。

- 备份服务器地址需为公网 IP 地址,并且入站安全组是放通状态,详情请参见 添加安全组规则 。
- 备份服务器通过 SSH 的方式进行备份,备份服务器设置成功后,系统每日02:00(UTC+8)定时备份上一天的数据到目标机器目录。

备份服务器设置	
备份服务器地址:	
备份服务器端口:	22
备份服务器用户名:	root
备份服务器密码:	
备份服务器目录路径	/data/beifen
备份开关:	Я
[保存

- 4. 设置完成后,数据安全审计管理系统中的数据将会按照设置路径进行备份。
- 5. (可选)如需恢复之前存在的数据,在备份服务器设置页面,单击【数据恢复】页签。
- 6. (可选)在数据恢复页签中,单击【数据恢复】,选择恢复日期并导入恢复数据即可。

数据恢复				Х	
恢复日期:	请选择日期	Ë	备份文件:	土 点击上传文件	
				关闭	

审计管理 安全审计与分析 审计数据

最近更新时间: 2025-05-27 16:30:32

审计概览

- 1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面,详情可参见 控制台登录 。
- 2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【安全审计与分析】>【审计概览】,即可进入审计概览页面。
- 在审计概览页面中,可总览全网数据库日志信息,态势分析,风险占比以及查询单个数据库资产详细信息,如需了解数据库资产审计详细内容,可在审计概览 页面下方查询详细信息。
 - 日志总数:用于统计全网各数据资产日志总数。
 - 今日日志:用于统计全网各数据资产今日日志总数。
 - 今日风险:用于统计全网各数据资产今日风险总数。
 - **今日会话:**用于统计全网各数据资产今日会话总数。
 - 态势分析:可查看您所配置的审计单元的审计趋势,风险趋势,会话趋势,还可按照高风险、中风险、低风险进行查看各个风险级别详细数据,每个报表 可展示三种走势图及三类风险级别数据:
 - **审计趋势**:用于展示数据资产的审计单元语句压力,展示时间有24小时、7天、30天。
 - 风险趋势:用于展示数据资产的审计单元高中低三类风险的统计信息,展示时间有24小时、7天、30天。
 - 会话趋势:用于展示数据资产的审计单元各类会话信息,展示时间有24小时、7天、30天。
 - 风险占比统计:用于显示数据资产对应的命中风险等级。
 - 风险等级:用于展示数据资产审计单元有关的自定义规则命中风险信息,展示时间有24小时、7天、30天。
 - 数据资产:用于展示被命中的数据资产,展示时间有24小时、7天、30天。
 - 资产审计:主要展示单个数据资产的会话总数,DDL 操作数量、失败会话数量、最大并发会话及风险数等信息。

日志总数	今日日志	今日风险		今日会语	
30.38万条	8.34万条	0 ↑		1.15 万次	
已运行 0 年 3 天 22 小时 空间使用: 期純血 18.5GB / 50GB 数据血 1.97GB / 197GB	日环比: 74% ▲ 陶环比: 183% ▲	日孫比: 0%▼	周环比: 0%▼	日頭比: 92%▲	周环社: 680% ▲
忽势分析 24小时	7天 30天 2021-03-10 ~ 2021-03-16 日	风险占比统计	24/187	7天 30天 2021-03-10 ~	2021-03-16
审计趋势 风险趋势 会活趋势		风险等级 数据资产			
		88. 792		ा वरीव तरफ बा वरीव तरफ बा वरीव दा	

日志检索

日志检索主要提供日志查询与导出功能。

- 1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面,详情可参见 控制台登录 。
- 2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【安全审计与分析】>【审计日志】,即可进入审计日志页面。
- 管理员通过 审计概览 定位到疑似有风险的数据库审计单元,或者企业网络已经发生数据库安全问题时,可在日志检索页面查询并导出日志信息。

*	(计组:		✓ 数据资产: 全部		数据资产类型: 全部				
R	2249-102 (E2	Utt	· 用户	×8i III6λ	命中现	B:			▲ 協 尋出 展开∨
	最近—小8f	今天 昨天 本周 上周	本月 上月 自定义						
	0 ±80	^{紀成,} 政策总量:2,925 条							
	序号	数据库用户	查户30P	1916日	命中规则	访问原	审计组名	风险够级	SQL语句
	1			01-13 17:14:24				- (6ERJ\$	
	2			01-13 17:14:09				- (ER)20	

日志查询

在日志检索页面,您可以按照审计单元、风险等级、用户名、命中规则及时间,对日志进行查询。



审计组:	∨数据资产	全部		数据资产类型:	全部			
风险等级: 中风险		用户名:	请输入			命中规则:	无	✓
最近一小时 今天 昨天 本周	上周 本月 上月 自定义							

查看数据详情

在日志列表中,可单击某条记录查看其详细内容。

i	第3条数据详情	
	操作语句:	
	操作类型:	INSERT
	操作时间:	01-06 17:25:03
	SessionID:	
	命中规则:	insert
	风险等级:	◎ 低风险
	数据库:	
	数据库IP:	
	数据库用户:	
	表名:	
	影响行数:	1
	执行时间:	0 ms
	返回消息:	
	返回码:	0
	审计组ID:	
	客户端IP:	
	访问源业务部门:	
	包长度:	
	使用工具:	
	终端名称:	
		关

日志导出

检索出需要导出的数据,现已支持不限数量导出,在列表上方单击【导出】,弹出导出数据弹窗,单击【确定】即可将数据导出,导出文件类型为 Excel(.xlsx 格式)。

⚠ 注意 尽量缩小导出范围,导出数量过多,会影响服务器性	È.
Excel文件生成	×
导出记录16,075,835条,确认要导出吗? 注:尽量缩小范围导出,导出数量过多,会影响服务性能	
取消	确定





规则配置

最近更新时间: 2025-05-27 16:30:32

规则配置可定义数据安全审计的审计单元的安全规则。数据安全审计具备两个默认规则,AI 引擎规则和 CVE 引擎规则,默认规则不可删除、不可编辑。下面将 为您详细介绍配置操作。

操作步骤

以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中,选择【安全审计与分析】>【规则配置】即可进入规则配置页面。

新建规则

如需自定义规则满足个性化审计需求,单击【添加规则】,进入新建规则页面,填写规则名称等,单击【保存】即可。

△ 注意

- 规则配置支持同一规则配置多个条件,多个条件之间为 "与"关系,必须全部匹配才能够触发规则和告警。
- 自定义规则默认为黑名单,触发后将产生告警并且记录入库。如果管理员需要节省数据安全审计的审计单元的存储空间,指定部分操作行为不记录不 入库,可在规则中指定相关操作后,选择"白名单"选项,并且将告警选项都取消。

以上操作完成后,即可实现白名单类型规则配置,减少误报、减轻数据安全审计的审计单元存储压力。

规则类型:	● 黑名单 ○ 白名单		
* 规则名称:	请输入规则名称		
	不超过15个中文字符长度,支持中文、英文以及		
涉及审计单元:	请选择审计单元		
规则备注:	选填		
		A 14	 47 //-
张件设置:	¥β	条件 、	操作
	添加		
危险等级:	低风险		
告警:			
	保存取消		

• 规则示例

在规则配置页面,单击【添加规则】,按下图配置规则,表名和阈值根据您的业务场景自行设定,单击【保存】即可。

规则名称:	请输入规则名称					
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~					
审计单元:	请选择审计单元					
规则备注:	选填					
条件设置:	字段		条件		值	操作
	表名(tb_name)		包含		xx_table	
	操作类型(sql_type)		包含		select	删除
	影响行数(effect_row)	~	大于等于	v	10	删除
	添加					
<b>己险等级</b> :	低风险					
危险等级:	任风险					

#### • 规则配置建议

以下三个建议规则仅作为示例,用户可根据自身业务自行配置。



### ○ 防爬取规则: 防止使用例如 select 操作语句,爬取表数据。

规则类型:	<ul> <li>● 黑名单 ○ 白名单</li> </ul>			
* 规则名称:	请输入规则名称			
	不超过15个中文字符长度,支持中文、英文以及			
涉及审计单元:	请选择审计单元			
规则备注:	选填			
条件设置:	字段	条件	值	操作
	操作类型(sql_type) V	<b>包</b> 含 ~ ~	select	
	影响行数(effect_row) ∨	大于等于	100	删除
	湊加			
危险等级:	低风险			
告警:				
	保存 取消			

### 注意 影响行数可以根据业务自行配置。

### ○ 慢查询发现规则:检查执行时间较长的 SQL 语句,便于进行优化。

* 规则名称:	请输入规则名称					
	、 不超过15个中文字符长度,支持中文、英文以	以及				
切下 ( ) 汲审计单元:	请选择审计单元					
规则备注:	选填					
条件设置:	字段		条件		值	操作
	操作类型(sql_type)	$\sim$	包含	~	select	
	执行时间(exec_time)		大于等于		500.00 毫秒	删除
	添加					
危险等级:	低风险					
告警:						
	保存取消					

执行时间可以根据业务自行配置。

○ 危险操作规则:检查执行 DELETE/DROP/ALTER 等类型的高危 SQL 语句。



* 观则省称	: 请输入规则名称			
	不超过15个中文字符长度,支持中文、英文	文以及		
步及审计单元	: 请选择审计单元			
规则备注	: 选填			
友供汎業	: 字段	条件	值	操
示计设直				
水件模直	操作类型(sql_type)	✓ 包含	✓ drop	
赤叶坡直	操作类型(sql_type) 添加	∨	✓ drop	
<b>水</b> 叶坡直	操作类型(sql_type) 添加	∨ 包含	✓ drop	

### 修改规则

在规则列表中,找到需要修改的规则,在右侧操作栏中,单击【修改】,修改信息后单击【保存】即可。

规则名称	涉及审计组	备注	操作
AI引擎	全部	系統内置规则	修改
CVE引擎	全部	系统内置规则	修改
_			修改 删除

## 删除规则

在规则列表中,找到需要删除的规则,在右侧操作栏中,单击【删除】,再单击询问窗【确定】即可。

	<ul> <li>您确认要删除吗?</li> <li>取 消</li> <li>确 定</li> </ul>
	修改 删除



## 审计报表

最近更新时间: 2025-05-27 16:30:32

审计报表功能主要展示所有配置过的审计组数据,并提供搜索、查看及 PDF 下载功能,具体操作步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【安全审计与分析】>【审计报表】,即可进入审计报表页面。

## 说明 如忘记登录密码,可以提交工单找回密码。

3. 在审计报表页面中,可查看内容包括报告名称、报告说明及发送目标等字段,同时可以进行相关操作,每个页面默认展示10条数据,可按照报告名称、生成方 式、开始时间及结束时间,对报告进行搜索,还可下载 PDF 报告。

新建报表						
报告名称:	生成方式: 全部 🗸	时间:开始日期	~ 结束日期 芭	搜索		
报表名称	报表说明	发送目标	报表生成时间	报表类型	状态	操作
审计日报_2021-03-15	日振		2021-03-15 21:00:02	定时生成	⊘ 已生成	查看 pdf下载 删除
报告_2021-03-14	1		2021-03-14 17:00:01	定时生成	⊘ 已生成	查看 pdf下载 删除
报告_2021-03-13	1		2021-03-13 17:00:02	迪时生成	⊘ 已生成	查看   pdf下载   删除

#### • 定时生成报表

数据安全审计管理系统支持定时生成报表。

在报表上方单击【新建报表】,弹出新建报表报表弹窗,选择"定时报表",并依次输入模板名称、统计周期(可选择定时执行、每天一次、每周一次、每月 一次)、执行时间(精确到时分秒)、报告说明,设置完成后,单击【确定】,即可在您设定的执行时间定时生成报表。

新建报表		$\times$
报告类型:	○ 即时报表 💿 定时报表	
* 模板名称:	审计日报 最多30个字符	
统计周期:	每天一次 🗸	
* 执行时间:	21:00:00 ① 注:建议导出时间为凌 晨1点	
* 报告说明:	日报	
	最多200个字符	
	取消 确	Ē

#### • 即时生成报表

数据安全审计管理系统支持即时生成报表,即生成某个时间段内的报表。

在报表上方单击【新建报表】,弹出新建报表弹窗,选择"即时报表",依次输入报告名称、审计单元、统计开始时间、统计结束时间、报告说明,单击【确 定】,即可输出您规定的时间范围内的报表。

⚠ 注意 开始时间应早于结束时间。



新建报表		×
报告类型:	● 即时报表 ○ 定时报表	
* 报告名称:	最多30个字符	
审计单元:		V
* 统计开始时间:	2021-03-15 00:00:00	
* 统计结束时间:	2021-03-15 23:59:59	Ë
* 报告说明:	最多200个字符	10
		取消 确定



## 数据资产与 Agent

最近更新时间: 2025-05-27 16:30:32

## Agent 配置

- 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】,即可进入审计用 Agent 页面。
- 2. Agent 部署。在审计用 Agent 页面,选择【Agent 配置】>【添加 Agent】,可配置审计 Agent 的各类参数并提供下载链接,配置步骤以及配置注意事项,请参见 Agent 部署。
- 3. 添加完成 Agent 后,在 Agent 配置页面,可查看所有已正确安装且能实现 DSA(Data Security Audit) 实例网络互通的 Agent 信息。

添加Agent				
Agent名称	审计服务IP	审计服务端口	数据库IP	操作
			详情	下载Linux Agent   下载Windows Agent   linux批量部署 🔞   自制除
			详情	下载Linux Agent   下载Windows Agent   linux批量部署 💿   自我除

列表各字段含义如下:

- Agent 名称:用于配置该 Agent 的名称。
- 审计服务 IP: Agent 回传数据的源 IP。
- 审计服务端口: 该 Agent 配置的审计端口。
- 数据库 IP: 单击【详情】可查看该 Agent 审计的数据库的所有 IP 地址。
- 审计 IP:用于显示该 Agent 配置的审计范围,由于 IP 范围内容较多,可单击【详情】进行阅览。
- 操作:用于下载该 Agent 的链接。
  - 单击【下载 Linux Agent】或【下载 Windows Agent】,弹出部署 IP 窗口,可以按 IP 部署或按 IP 段部署(IP 段支持全段审计),单击【确 定】即可开始下载 Agent。

#### ▲ 注意

- 若部署机器操作系统 CentOS 版本号小于7 或者 Ubuntu 版本号小于11,必须勾选下方说明,否则无法部署 Agent。
- 请添加安装包需要部署机器的 IP 或 IP 列表。
- 如未添加 IP 信息却部署了会导致 Agent 无法启动。
- 如有新的机器要部署请重新下载安装包并填写机器的 IP 信息。

部署IP	Х
<ul> <li>部署机器操作系统centos版本号小于7或者ubuntu 部署机器操作系统centos版本号小于7或者ubuntu版本号小于1 无法部署agent)</li> </ul>	版本号小于11 (注: 若 I,必须勾选此选项,否则
	取消 确定

○ 单击【删除】,可删除该条 Agent 信息。

#### 审计列表

- 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【审计用 Agent】>【审计列表】,即可进入审计列表中。
- 2. 在审计列表中,可以查看所有已配置的 Agent。审计列表默认展示内容包括:deployMac、部署服务器 IP、审计服务、部署状态、Agent 状态、系统类型、部署时间运行时长及相关操作。
  - 搜索:您可以按照部署状态、Agent 状态、审计服务 IP、Port (端口)对 Agent 进行搜索。。
  - 查看 Agent 配置详情:在"审计服务"栏中,单击【Agent 配置详情】,可以查看 Agent 配置相关信息。



○ 相关操作:在右侧操作栏,可以对 Agent 进行启动、停止、卸载、删除的相关操作。

部署状态: 全部 🗸 🗸	部署IP:	Agentitis:	全部 ∨	搜索				
deployMac	部署服务器IP	审计服务	部署状态	Agent状态	系统类型	部署时间	运行时长	操作
		[Agent配置详情]	部署完成	正常	linux	2020-12-29 20:32:01	13天14时40分10秒	启动   <b>停止   卸载   删</b> 除
		:[Agent配置详情]	部署完成	正常	linux	2020-12-28 11:48:02	2天0时36分13秒	启动   <b>停止   卸載   删除</b>
		Agent配置详情)	部署完成	高线: 网	linux	2020-12-23 11:18:02	0秒	启动 停止 卸戦 删除





最近更新时间: 2025-01-10 19:17:22

审计单元配置可为从属于一个应用的一台或多台数据库服务器进行命名,方便后续规则配置或审计信息时,使用直观的名字来表达数据库信息,优化策略和报表可 读性。下面将为您详细介绍配置操作。

- 1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面,详情可参见 控制台登录。
- 2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【配置管理】>【审计单元】,即可进入审计单元配置页面。

	<b>!) 说明</b> 若审计 Agent 部署	成功,会默认添加审计单元,无需自己新建。	
3.	在审计单元列表中,找到需	需要修改的审计单元(建议以业务应用名称为基础命名),在右侧操作栏单击【编辑】,在弹框中修	<b>8改信息后,单击【确定】即可</b> 。
	修改审计单元	X	
	* 审计单元名称: * 数据资产实例: 业务名: * 备注信息:		
		取消 确定	



## 访问源配置

最近更新时间: 2025-05-27 16:30:32

访问源配置可为从属于同一部门或同一网络区域的访问 IP 段进行命名,方便后续规则配置、审计信息通过直观命名标识数据库访问端来源,优化策略以及报表可 读性。下面将为您详细介绍配置操作。

以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【配置管理】>【访问源】,即可进入访问源配置列表页面。

• 添加访问源

单击列表上方【添加】,在弹出窗口中,填写业务名、访问源名称、访问源包含 IP 段、备注信息,单击【确定】即可。

如未找到相应业务,可点	原击这里添加	
请输入访问源名称		
起始IP	结束IP	操作
0.0.0.1	255.255.255.254	
增加		
请输入备注信息		
		取消 确式
	如未找到相应业务,可/ 请输入访问源名称 起始IP 0.0.0.1 请输入备注信息	如未找到相应业务,可点击这里添加 请输入访问源名称 起始IP 结束IP 0.0.0.1 255.255.254 雪加

#### • 修改访问源

在访问源列表中,找到需要修改的访问源,在右侧操作栏中,单击【修改】,在弹框中修改信息后,单击【确定】即可。

影改访问源			×
• 业务名			
	如未找到相应业务,可点	击这里添加	
•访问源名称	:		
访问源包含IP段	: 起始IP	结束IP	操作
	127.0.0.1	127.255.255.254	
	墙加		
* 备注信息	: ds		
			取消 确定

#### • 删除访问源

在访问源列表中,找到需要删除的访问源,在右侧操作栏中,单击【删除】,再单击询问窗中的【确定】即可。

访问源名称	包含IP段数量	部门及业务名	备注	您确认要删除吗?
	1		ds	取消 确定
	1		ds	修改删除



## 部门业务配置

最近更新时间: 2025-01-10 19:17:22

#### 部门业务配置功能主要是部门配置与业务配置的相关功能,具体配置步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中,选择【配置管理】>【部门&业务】,即可进入部门业务配置页面。

1	说明				
	如忘记登录密码,	可以	提交工单	找回密码。	

- 3. 在部门业务配置页面,可进行部门配置及业务配置。
- 部门配置
  - 3.1 在部门业务配置页面,单击【部门配置】,可添加并查看部门名、部门负责人及备注,同时可进行相关操作。

部门配置 业务配置			
+ 添加部门 📋 删除			
部门名	部门负责人	备注	操作
test	小李		修改 删除
it运营部	马忠义		修改 删除
财务部	王五		修改 删除
采购部	赵四		修改 删除

3.2 在部门设置页面,单击【添加部门】,在弹出的添加部门窗口中,填写部门名、部门负责人以及备注信息,单击【确定】即可完成添加。

添加部门	×
. 如门夕.	1246 \ 47/7-F
* 라이 나는 :	「「「「「」」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」、「」、」、「」、
★部门负责人:	请输入部门负责人
备注信息:	请输入备注信息
	取消 确定

3.3 添加完成后,已添加的部门将出现在部门配置列表中,支持对已添加的部门进行修改或删除,且支持对部门信息批量选择删除。

部门曹	記置 业务配置			
+ 添	加部门 ① 删除			
	部门名	部门负责人	备注	操作
	test	小李		修改 删除
	it运营部	马忠义		修改 删除



○ 修改

找到需要修改的部门信息,在右侧操作栏单击【修改】,在弹出框中可以修改对应部门信息。

- 删除
- **方式1**: 找到需要删除的部门信息,在右侧操作栏单击【删除】,在弹出框中确认删除,即可完成删除。
- 方式2:选择需要删除的部门,在列表上方单击【删除】,即可批量删除部门信息。

### • 业务配置

3.1 在部门业务配置页面,单击【业务配置】,可添加并查看业务名、业务负责人、部门名及备注,同时可进行相关操作。

部门酉	部门配置 业务配置								
+ 漆	+ <b>添加业务</b> □ 删除								
	业务名	业务负责 人	部门名	备注	操作				
	test	小赵	test		修改 删除				
	薪资结算系统	meller	财务部	18	修改 删除				

3.2 在业务配置页面,单击【添加业务】,在弹出的添加业务窗口中,填写部门名、业务名、业务负责人以及备注信息,填写完成后,单击【确定】即可完成 添加。

添加业务		$\times$
*部门名:		$\sim$
* <u>业</u> 务名:	请输入业务名	
* 业务负责人:	请输入业务负责人	
备注信息:	请输入备注信息	
	取消	确定

3.3 添加完成后,已添加的业务将出现在业务配置列表中,支持对已添加的业务进行修改或删除,且支持对业务信息进行批量选择删除。

部门督	部门配置 业务配置									
+ 漆	+ 添加业务 ① 删除									
	业务名	业务负责 人	部门名	备注	操作					
	test	小赵	test		修改 删除					
	薪资结算系统	meller	财务部		修改 删除					

- 修改
  - 找到需要修改的业务信息,在右侧操作栏单击【修改】,在弹出框中可以修改对应业务信息。
    - 删除
      - 方式1: 找到需要删除的业务信息,在右侧操作栏单击【删除】,在弹出框中确认删除,即可完成删除。
      - **方式2**:选择需要删除的业务,在列表上方单击【删除】,在弹出框中确认删除,即可批量删除业务信息。



## 操作日志管理

最近更新时间: 2025-01-10 19:17:22

操作审计员负责审计数据安全审计各管理员的操作,防止其他管理员滥用职权进行非法操作。用操作管理员账号登录后,能够阅览管理员操作日志列表并对行为规 则进行配置。

### 日志检索

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以操作管理员账号登录操作日志页面,在左侧导航栏中单击【行为规则配置】,即可进入操作日志页面。

① <b>说明</b> 如忘记登录密码,可以 提交工单 找回密码。	
--------------------------------------	--

3. 在操作日志页面,您可以根据操作账户、操作 IP、行为分类、操作时间检索还原非法操作完整信息。

操作日志							
操作帐户:	操作IP:	行为分类:	全部 ^	、 操作时间:	开始日期 ~ 结束日期 🖻	搜索	
操作时间	操作则	行	王部 登录 退出		操作IP	行为分类	操作行为
2018-05-25 11:28:36	userad	lmin	新增配置 修改配置		14.17.22.33	检察日志	检索日志
2018-05-25 11:28:35	userad	łmin	删除配置 检索日志		14.17.22.33	检索日志	日志检索
2018-05-25 11:28:34	userad	lmin	导出报告	*	14.17.22.33	检索日志	日志检索

### 行为规则配置

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以操作管理员账号登录操作日志页面,在左侧导航栏中单击【行为规则配置】,即可进入行为规则配置页面。



 在行为规则配置页面,可以查看行为操作、行为分类、告警模板、备注、是否开启告警及相关操作,同时可按照行为分类、行为操作及危险等级,对行为规则 进行搜索。





行为	5分类: 全部	∨ 行为操作:	全部 🗸	危险等级: 全部	✓ 搜索		
	行为操作	行为分类	告警模版	备注	危险等级	是否开启告警	操作
	登录	用户登录	报告,有敌人来了,.		低级>	开启	修改
	修改密码	用户登录			低级>	●关闭	修改

#### 字段说明:

- 行为操作:用户对系统各个账户的功能操作。
- 行为分类:用户对系统功能操作所属的模块名
- 告警信息模板: 用户执行操作时邮件所发送的告警内容
- 备注:用户对行为规则的进一步说明。
- 危险等级:对用户操作行为的评级,可设置行为危险等级,包括低级、中级及高级。
- 是否开启告警:用户开启后,触发行为规则审计,则会发送告警信息,关闭后,只会记录操作,不会发送告警信息。
- 操作:在目标行为右侧操作栏,单击【修改】,即可对行为操作信息进行修改。

修改配置			×
行为操作:	登录		
行为分类:	用户登录		
接口路由:			
告警信息模板:	报告,有敌人来了,请注意,小心敌方陷阱		
备注:			Ĩ
			4
危险等级:	1比较	~	
是否开启告警:	●关闭		
		取消 确知	Ē



# v5.0.6 系统管理 系统资源监控

最近更新时间:2025-01-10 19:17:22

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。



2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【系统资源监控】,即可进入资源监控页面,该页面包括系统详细信息、系统存储空间统计和流量走势实时统计。

```
() 说明
```

如忘记登录密码,可以 提交工单 找回密码。

#### ○ 系统详细信息

系统详细信息包含系统产品名称、产品规格、当前版本等基础信息,以及数据安全审计总审计组数参数信息。

系统详情	
产品名称	重启
产品规格	
当前版本	
连续运行时长	0年3月13天5小时21分11秒
系统当前时间	2021-04-22 16:39:57
购买峰值流量	3000 QPS
已用/总审计组数	牧2/3个
自定义规则数	2个

### ○ 系统存储空间统计

存储空间统计用于展示数据安全审计实例当前的存储状态。在系统存储空间统计右上角,单击【清理剩余空间】,将清理的数据包含所选的日期。例如, 选择了12月1日至12月3日,则会删除12月1日、2日、3日,3天的数据。

#### 🕛 说明

统计报表将磁盘空间分为四个类型:

- 剩余空间:数据安全审计实例存储剩余空间;
- 系统占用空间: 数据安全审计自身代码所占存储空间;
- 审计日志占用空间: 数据安全审计记录的数据库操作信息日志占用空间;
- 其他占用空间:数据安全审计实例其他代码、配置文件占用空间。





#### ○ 流量走势实时统计

流量走势实时统计能统计一定时间跨度(最近30分钟、最近24小时、最近7天)内数据安全审计中所审计的所有数据库的 QPS,确认全网 QPS 峰值是 否超过购买峰值,以帮助管理员了解数据安全审计性能状况,及时扩容升级产品。





## 用户管理

È

最近更新时间: 2025-05-27 16:30:32

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中单击【用户管理】即可进入用户页面。

<ol> <li>说明 如忘记登录</li> </ol>	<b>录密码,可以 提交工单</b> :	找回密码。						
○ <b>查看账号信</b> 第 账号管理用于	<b>息</b> 于管理 DSA 实例所有账	号。系统管理员可以	通过列表查看所有	账号信息,包捂	師属角色、真实	<b>实姓名、创</b> 建	皆期以及联系方	式等。
<ol> <li>说明</li> <li>OTP</li> <li>管理5</li> </ol>	[,] 二维码:如需开启 OTF 员账号下的 OTP 验证,	^{&gt;} 实现登录双重验证 单击【 OTP 验证】	,可在相应账号右侦 ,查看原图并扫描	则操作栏,单击 动态校验码。	【OTP二维码】	,或在数据	安全审计管理页	面右上角,找到
- 転号名称	所漏角色 平 真实姓名 创建	日期 创建人	最后修改人 最后修改时间	联系方式	登录IP范围 摄	R/T		
sysadmin	系统管理员 2020	-09-28 10:00 系統款认创建	/ 2020-10-20 16:52	电话: 邮稿: 你信:	1740a B	DTP二编码 编辑		
useradmin	审计管理员 2020	-09-28 10:00 3549.001.0138	/ 2020-09-28 10:00	电流: 邮稿: 即他:	9410 C	DTP二條码 自規		
○ <b>添加账号</b> 如需要增加管	管理员账号,单击【添加	账号 】 ,在弹框中填	写账号信息,选择	所属角色后,单	自击【确定】即可	J.		
* 账号:								
* 密码:								
* 真实姓名:								
* 手机号码:								
* 由『释音:								
* 微信号:								
* 所属角色:	审计管理员		~					
登录IP范围:	起始IP	结束IP	操作					
	0.0.0.1	255.255.255.255						
	添加 (当ip为ipv6格式时,仅对	超始(P有效)						

取消 确定



### ○ 修改和删除账号

如需对账号进行修改或删除,可在相应账号操作列单击【编辑】或【删除】对账号进行调整。

注意     系统默认创建账号不可删除。
----------------------

帐号名称	所還角色	平 真实姓名	创建日期	创建人	最后核改人	最后修改时间	联系方式	登录IP范围	操作
sysadmin	系统管理员		2020-09-28 10:00	系统就认创建	T	2020-10-20 16:52	电话: 邮通: 微信:	17 (B)	OTP二编码 机5】
useradmin	市计管理员		2020-09-28 10:00	斯统默认创建	1	2020-09-28 10:00	电话: 邮稿: 网络:	17 M	OTP二维码 時間
sysaudit	操作审计管理员		2020-09-28 10:00	系统就认识能	7	2020-09-28 10:00	电话: 邮稿: 微信:	¥10	OTP二维码 调辑
-	审计管理员	100	2020-11-12 11:45	sysadmin	T	2020-11-12 11:45	电话: 1 邮编:	详细	OTP ^一 维码 编辑 删除



## OTP 设置

最近更新时间: 2025-05-27 16:30:32

本文档将为您介绍如何开启 OTP 校验,并通过 OTP 校验登录数据安全审计管理页面。

### 操作步骤

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【OTP 设置】,即可进入 OTP 设置页面。



3. 在 OTP 设置页面,设置校验开关,如需开启 OTP 验证选项,选中开启 OTP 验证,根据提示扫描 OTP 码,输入正确的 OTP 码,单击【确定】,退出登 录系统即可。



OTP设置	
	校验开关: • 开启OTP验证 关闭OTP验证
	12 Tr

4. 再次登录数据安全审计管理页面,需要输入OTP 校验码。





## 告警设置

最近更新时间: 2025-01-10 19:17:22

告警支持针对每个审计规则策略进行告警,告警支持邮件告警、syslog 告警,具体操作步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,在右侧操作栏,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【告警设置】,即可进入告警设置页面。

## 说明 如忘记登录密码,可以提交工单找回密码。

3. 在告警设置页面,分别对告警开关、系统资源告警配置、syslog 告警配置及邮件告警配置功能进行设置。

#### ○ 告警开关

在告警设置页面,单击【告警开关】,分为【告警方式】和【告警内容】,打开需要开启告警的选项,单击【提交】,即可对 syslog 告警配置 中所设置 的服务器进行监控,且当满足告警条件时,将触发告警,并发送邮件至您所 配置的告警邮箱 中。

# ⑦ 注意 若需要接收告警信息,需打开邮件告警开关,且已在 邮件告警配置 中设置告警接收邮箱,否则无法接收告警信息。

系统资源古警配置	syslog舌警配置	邮件音警配置	
部件音警: 77			syslog쑴蒈: (캐)
QPS告答: <mark>开</mark> )			sql风险告警: 开
系统资源告答: 开 🔵			行为规则告答: 开
agent掉线告警: 开			
提交			
	系統資源吉容配置 邮件告容: 第 QPS告答: 第 系統資源告容: 第 agent掉线告答: 第 提 又	系统资源告望配置 syslog古智配置 邮件告答: 并 QPS告答: 并 系统资源告答: 并 agent操线音答: 并 提交	<ul> <li>系统资源苦馨社園</li> <li>syslog古馨社園</li> <li>部件告答: (1)</li> <li>QPS告答: (1)</li> <li>系統資源告答: (1)</li> <li>agent挿誌告答: (1)</li> <li>送文</li> </ul>

#### ○ 系统资源告警配置

在告警设置页面,单击【系统资源告警配置】,设置系统资源告警的触发条件,可将磁盘、内存、CPU 负载在0 - 100%之间调整,可自定义带宽值,单



#### 击【提交】,即可对 syslog 告警配置 中所设置的服务器进行监控。



#### ○ syslog 告警配置

## ▲ 注意 目前 syslog 告警服务只支持 TCP 协议。

在告警设置页面,单击【syslog 告警配置】,输入需要记录的 syslog 服务器 IP 和端口,单击【提交】,即可完成 syslog 告警条件配置,设置完成 后将监控所配置的服务器。

系统资源告警配置	syslog告警配置	邮件告警配置
* syslog服务器:		
* 端口: [		
	测试 提交	注: 目前syslog告警服务只支持tcp

#### ○ 邮件告警配置

单击【邮件告警配置】,依次填入邮件服务器的相关配置信息,如需添加多个收件人,请以英文分号分隔,填写完成后,单击【提交】,当满足告警条件 时,将发送邮件至所配置的邮箱中。

⚠	注意				
	若填写 QQ 邮箱账号,	密码需填写所设置的邮箱密码。			



告警开关	系统资源告答配置 syslog告答配置 邮件告答配置	
* SMTD肥念题。		
51011 (BC) 88	第三方邮件服务容易受服务器反垃圾机制影响,如遇到不可用的, 建议尝试切换其他邮件服务	
* 端口:		
* 邮件账号:		
* 密码:	:	
* 发件人:	此密码非邮箱登录密码	
收件人:	1	
	多个收件人请以分号;分隔	
SSL		
	测试 提交 重置	



# 时间服务器

L

重置

最近更新时间: 2025-05-27 16:30:32

时间服务器主要用于同步时间,找到您需要同步时间的服务器 IP 进行设置即可,具体操作步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,在右侧操作栏,单击【管理】,进入数据安全审计登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 使用 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【时间服务器】,即可进入时间服务器设置页面。

	() <b>说明</b> 如忘记登录密码,可以 提交工单 找回密码。	
3.	在时间服务器设置页面,输入 NTP 服务器 IP,单击【提交】,即可完成设置。	
	时间服务器设置	
	* NTP服务器IP: 诸输入NTP服务器IP	

4. 设置完成后,数据安全审计系统时间会与您设置的 NTP 服务器地址所在时间进行同步。



## 备份服务器

最近更新时间: 2025-05-27 16:30:32

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【备份服务器设置】,即可进入备份服务器设置页面。

<ol> <li>说明 如忘记登录密码,可以提交工单找回密码。</li> </ol>	
------------------------------------------------	--

在备份服务器设置页面,依次输入备份服务器地址、备份服务器端口、备份服务器用户名、备份服务器密码、备份服务器目录路径,打开备份开关,单击【保存】即可完成备份服务器设置。

	说明
~	W U PV J

- 备份服务器地址需为公网 IP 地址,并且入站安全组是放通状态,详情请参见 添加安全组规则 。
- 备份服务器通过 SSH 的方式进行备份,备份服务器设置成功后,系统每日02:00(UTC+8)定时备份上一天的数据到目标机器目录。

备份服务器设置	
备份服务器地址:	
备份服务器端口:	22
备份服务器用户名:	root
备份服务器密码:	
备份服务器目录路径	/data/beifen
备份开关:	Я
[	保存

- 4. 设置完成后,数据安全审计管理系统中的数据将会按照设置路径进行备份。
- 5. (可选)如需恢复之前存在的数据,在备份服务器设置页面,单击【数据恢复】页签。
- 6. (可选)在数据恢复页签中,单击【数据恢复】,选择恢复日期并导入恢复数据即可。

数据恢复				Х	
恢复日期:	请选择日期	Ë	备份文件:	土 点击上传文件	
				关闭	

# 审计管理 安全审计与分析 审计数据

最近更新时间: 2025-05-27 16:30:32

## 审计概览

- 1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面,详情可参见 控制台登录 。
- 2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【安全审计与分析】>【审计概览】,即可进入审计概览页面。
- 在审计概览页面中,可总览全网数据库各类排行信息以及查询单个数据库实例概览信息,如需了解数据库审计组详细内容,可在审计概览页面下方查询审计组 的详细信息。
  - 数据库排行统计:上方条形统计图为数据库排行,排行统计数据内容如下:
    - **风险排行**:用于统计全网各数据库风险总数,降序排列。
    - **语句压力排行**:用于统计全网各数据库语句压力总数,降序排列。
  - 审计组详情: 审计组详情内可查看您所配置的审计组的风险分布 Top5、语句压力统计 Top5(QPS),会话分布 Top5,还可按照全部、高风险、中风 险、低风险进行查看各个风险级别详细数据,每个报表可展示三种走势图及三类风险级别数据:
    - 风险分布:用于展示本数据库审计组高中低三类风险的统计信息,展示时间范围可在1天到365天之间进行调整。
    - 自定义规则命中:用于展示与本数据库审计组有关的自定义规则命中信息,展示时间范围可在1天到365天之间进行调整。
    - 语句压力统计:用于展示本数据库审计组语句压力的统计信息,展示时间范围可在1天到365天之间进行调整。
    - 会话统计:用于展示本数据库审计组各类会话信息,展示时间范围可在1天到365天之间进行调整。

审计组详情 TOP5	V I				[	(天 7天 30天 90天 6个月 1年)
风险分布TOP5		申计空机系统 -〇- 审计签到系统	审计工作服乐购基线			
80000 - 50000 - 40000 -						
20000 -	and and the second and a second					
0.00 00:00 04-02	06:00 04-02	12:00 04-02	18:00 04-02	23-59 04-02		
		12/09	1960	2249		
64.62 会运分布TOP5	04.62 0- #HRIKR -0- #HRIKR 10- #HRIKR -0- #HRIKR 10- #HRIKR -0- #HRIKR	04-02 *++₩9₩60,*++T	04-02 (金田) 新福井 村田元本成本(一) 東小村港市電車の	64-02		
0.00 00.00 04-02	06.00 04-02	12:00 04-02	18:00 04-02	23-59 04-02		

## 日志检索

日志检索主要提供日志查询与导出功能。

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面,详情可参见 <mark>控制台登录</mark> 。

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【安全审计与分析】>【审计日志】,即可进入审计日志页面。



3. 管理员通过 审计概览 定位到疑似有风险的数据库审计组,或者企业网络已经发生数据库安全问题时,可在日志检索页面查询并导出日志信息。

审计组:		✓ 数据资产: 全部		数据资产类型: 全部				
风险等极:	积险	· 用户	Bi IBAA	命中规则	ti 📃 🔻			▲ 湖 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
最近—小时	今天 昨天 本周 上月	1 本月 上月 自地义						
Ø ±0	日完成,数据总量:2,925 条							
19-10	数据库用户	衛/ ^{pi} JAIP	PIE	命中规则	访问原	审计组名	风险等级	SQL语句
1			01-13 17:14:24				- (16R3b)	
2			01-13 17:14:09				- (ERIP)	

### 日志查询

在日志检索页面,您可以按照审计组、风险等级、用户名、命中规则及时间,对日志进行查询。

审计组:		数据资产:	全部		数据资产类型:	全部		
风险等级:	中风险		用户名:	请输入		命中规则	无	宮岡 导出 履开マ
最近一小	时 今天 昨天 本周 上周 本月 上月	自定义						

#### 查看数据详情

在日志列表中,可单击某条记录查看其详细内容。

<b>(</b> )	第6条数据详情	
	操作语句:	
	操作类型:	
	操作时间:	01-12 10:56:28
	SessionID:	
	命中规则:	
	风险等级:	• 正常
	数据库:	
	数据库IP:	
	数据库用户:	root
	表名:	
	影响行数:	
	执行时间:	
	返回消息:	
	返回码:	
	审计组ID:	
	客户端IP:	
	访问源业务部门:	
	包长度:	
	使用工具:	
	终端名称:	
		关闭

## 日志导出

检索出需要导出的数据,现已支持不限数量导出,在列表上方单击【导出】,弹出导出数据弹窗,单击【确定】即可将数据导出,导出文件类型为 Excel(.xlsx 格式)。









## 规则配置

最近更新时间: 2025-05-27 16:30:32

规则配置可定义数据安全审计的审计组的安全规则。数据安全审计具备两个默认规则,AI 引擎规则和 CVE 引擎规则,默认规则不可删除、不可编辑。下面将为 您详细介绍配置操作。

### 操作步骤

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中,选择【安全审计与分析】>【规则配置】即可进入规则配置页面。

#### 新建规则

如需自定义规则满足个性化审计需求,单击【添加规则】,进入新建规则页面,填写规则名称等,单击【保存】即可。

### △ 注意

- 规则配置支持同一规则配置多个条件,多个条件之间为"与"关系,必须全部匹配才能够触发规则和告警。
- 自定义规则默认为黑名单,触发后将产生告警并且记录入库。如果管理员需要节省数据安全审计的审计组的存储空间,指定部分操作行为不记录不入 库,可在规则中指定相关操作后,选择"白名单"选项,并且将告警选项都取消。

以上操作完成后,即可实现白名单类型规则配置,减少误报、减轻数据安全审计的审计组存储压力。

规则类型:	● 黑名单 ○ 白名单				
* 规则名称:	请输入规则名称				
	不超过15个中文字符长度	,支持中文、英文以及			
涉及审计组:	请选择审计组				
规则备注:	洗填				
条件设置:	字段	条件	值	操作	
	▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲	v			
	添加				
危险等级:	低风险				~
告警:					
	保存取消				

#### • 规则示例

在规则配置页面,单击【添加规则】,按下图配置规则,表名和阈值根据您的业务场景自行设定,单击【保存】即可。



名称:	请输入规则名称			
7	不超过15个中文字符长度,支持中	文、英文以及		
†组:	请选择审计组			
注:	选填			
2置: 5	字段	条件	值	操作
	表名(tb_name) V	包含	<ul> <li>✓ xxx_test</li> </ul>	
	SQL类型(sql_type) V	包含	<ul> <li>✓ select</li> </ul>	<b>新時</b>
	影响行数(effect_row) 🛛 🗸	大于等于	✓ 50	删除
3	秦加			
<i>奏</i> 级:	任风险			

#### • 规则配置建议

以下三个建议规则仅作为示例,用户可根据自身业务自行配置。

○ 防爬取规则:防止使用例如 select 操作语句,爬取表数据。

<u>へ</u> 注 影	。 向行数可以根据业务自行配置	<u>ڦ</u> ر		
规则类型:	● 黑名単 ○ 白名単			
•规则名称:	防爬取策略			
	不超过15个中文字符长度,支持中文、英	这以及		
涉及审计组:	test ×			
规则备注:	选填			
条件设置:	字段	条件	值	操作
	SQL类型(sql_type) V	<b>包含</b> >>	select	
	影响行数(effect_row) 🗸	大于等于	100	删除
	満加			
危险等级:	低风险			
告警:				
	保存取消			
慢查询发	<b>见规则</b> :检查执行时间较长的	的 SQL 语句,便于进行优化	0	

▲ 注意				
执行时间可以根据业务自行配置。	o			



* 规则名称: 请输入规则名称: 请输入规则名称: 不超过15个中文						
不超过15个中文						
	子付衣皮,文符中义、央又以及					
步及审计组: 请选择审计组						
规则备注: 选填						
条件设置: 字段			条件	值		操作
操作类型(sql_t	ype)			select		
执行时间(exec	_time)	$\sim$	大于等于	500.00	毫秒	删除
添加						
危险等级: 低风险						

○ 危险操作规则:检查执行 DELETE/DROP/ALTER 等类型的高危 SQL 语句。

规则名称:				
	不超过15个中文字符长度,	支持中文、英文以及		
及审计组:	test ×			
	244-875			
和4天了留7主;	2544			
条件设置:	字段	条件	值	操作
	SQL类型(sql_type)	∨ 包含	V drop	
	添加			
危险等级:	低风险			
æ. 25.				
古警:				

### 修改规则

在规则列表中,找到需要修改的规则,在右侧操作栏中,单击【修改】,修改信息后单击【保存】即可。

-			修改 删除
CVE引擎	全部	系统内置规则	修改
AI引擎	全部	系统内置规则	修改
规则名称	涉及审计组	备注	操作

## 删除规则

在规则列表中,找到需要删除的规则,在右侧操作栏中,单击【删除】,再单击询问窗【确定】即可。

	<ul> <li>您确认要删除吗?</li> <li>取 消</li> <li>确 定</li> </ul>
	修改 删除



## 审计报表

最近更新时间: 2025-05-27 16:30:32

审计报表功能主要展示所有配置过的审计组数据,并提供搜索、导出及 PDF 下载功能,具体操作步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【安全审计与分析】>【审计报表】,即可进入审计报表页面。

()	说明		
	如忘记登录密码,	可以 提交工单	找回密码。

3. 在审计报表页面中,可查看内容包括报告名称、报告说明及发送目标等字段,同时可以进行相关操作,每个页面默认展示10条数据,可按照报告名称、生成方 式、开始时间及结束时间,对报告进行搜索,还可下载 PDF 报告。

◎ 定时生成报表	區 即时生成报表						
报告名称:	生成方式: 全部	∨ 开始时间:	请选择日期	结束时间:	请选择日期	Ë	搜索
报告名称	报告说明	发送目标	报告生成时间	生成方式	状态	操作	
定时_2020-04-20	测试定时day1911	sysadmin	04-20 19:11	定时生成	已生成	查看 pdf	下载删除
定时_2020-04-20	测试定时month	sysadmin	04-20 16:10	定时生成	已生成	查看 pdf	下载 删除

#### • 定时生成报表

数据安全审计管理系统支持定时生成报表,在报表上方单击【定时生成报表】,弹出定时生成报表弹窗,依次输入模板名称、统计周期(可选择定时执行、每 天一次、每周一次、每月一次 )、执行时间(精确到时分秒 )、报告说明,设置完成后,单击【确定】,即可在您设定的执行时间定时生成报表。

定时生成报	表	$\times$
* 模板名称:	审计日报 最多30个字符	
统计周期:	每天一次 🗸	
* 执行时间:	02:00:00 ① 注: 建议导出时间为凌 晨1点	
* 报告说明:	dsa	
	最多200个字符	
	取消 确	定

#### • 即时生成报表

数据安全审计管理系统支持即时生成报表,即生成某个时间段内的报表,单击【即时生成报表】,依次输入报告名称、统计开始时间、统计结束时间、报告说 明,单击【确定】,即可输出您规定的时间范围内的报表。

开始时间应早于结束时间。



即时生成报表		×
* 报告名称:	最多30个字符	
* 统计开始时间:	2020-04-12 00:00:00	Ë
* 统计结束时间:	2020-04-12 23:59:59	Ë
* 报告说明:		1
	最多200个字符	
		取消 确定



# 数据资产与 Agent

最近更新时间: 2025-05-27 16:30:32

本文档将为您介绍如何部署审计 Agent,并指导您操作审计列表。

## Agent 配置

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

- 2. 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】,即可进入审计用 Agent 页面。
- 3. Agent 部署。在审计用 Agent 页面,选择【Agent 配置】>【添加 Agent】,可配置审计 Agent 的各类参数并提供下载链接,配置步骤以及配置注意事项,请参见 Agent 部署。
- 4. 添加完成 Agent 后,在 Agent 配置页面,可查看所有已正确安装且能实现 DSA(Data Security Audit) 实例网络互通的 Agent 信息。

添加Agent				
Agent名称	审计服务IP	审计服务端口	数据库IP	操作
			详情	下载Linux Agent   下载Windows Agent   linux批量部署 🔞   自義除
			详情	下载Linux Agent   下载Windows Agent   linux批量部署 🛞   自删除

列表各字段含义如下:

- Agent 名称:用于配置该 Agent 的名称。
- 审计服务 IP: Agent 回传数据的源 IP。
- 审计服务端口: 该 Agent 配置的审计端口。
- 数据库 IP: 单击【详情】可查看该 Agent 审计的数据库的所有 IP 地址。
- 审计 IP:用于显示该 Agent 配置的审计范围,由于 IP 范围内容较多,可单击【详情】进行阅览。
- 操作:用于下载该 Agent 的链接。
  - 单击【下载 Linux Agent】或【下载 Windows Agent】, 弹出部署 IP 窗口,可以按 IP 部署或按 IP 段部署(IP 段支持全段审计),单击【确 定】即可开始下载 Agent。

### △ 注意

- 若部署机器操作系统 CentOS 版本号小于7 或者 Ubuntu 版本号小于11,必须勾选下方说明,否则无法部署 Agent。
- 请添加安装包需要部署机器的 IP 或 IP 列表。
- 如未添加 IP 信息却部署了会导致 Agent 无法启动。
- 如有新的机器要部署请重新下载安装包并填写机器的 IP 信息。

部署IP	Х
部署机器操作系统centos版本号小于7或者ubunt 部署机器操作系统centos版本号小于7或者ubuntu版本号小于 无法部署agent)	iu 版本号小于11 (注: 若 F11, 必须勾选此选项, 否则
	取消 确定

○ 单击【删除】,可删除该条 Agent 信息。


## 审计列表

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

- 2. 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【审计用 Agent】>【审计列表】,即可进入审计列表中。
- 3. 在审计列表中,可以查看所有已配置的 Agent。审计列表默认展示内容包括:deployMac、部署服务器 IP、审计服务、部署状态、Agent 状态、系统类型、部署时间运行时长及相关操作。
  - 搜索:您可以按照部署状态、Agent 状态、审计服务 IP、Port (端口)对 Agent 进行搜索。
  - 查看 Agent 配置详情:在"审计服务"栏中,单击【Agent 配置详情】,可以查看 Agent 配置相关信息。
  - 相关操作:在右侧操作栏,可以对 Agent 进行启动、停止、卸载、删除的相关操作。

部署状态: 全部 V	部署IP:	Agent状态:	全部 ∨	搜索				
deployMac	部署服务譜IP	审计服务	部署状态	Agent状态	系统类型	部署时间	运行时长	操作
		(Agent配置详确)	部署完成	正業	linux	2020-12-29 20:32:01	13天14时40分10秒	启动   <b>停止   卸載   删</b> 除
		:[Agent配置详情]	部署完成	正常	linux	2020-12-28 11:48:02	2天0时36分13秒	启动   停止   卸载   删除
		Agent配置详情)	部署完成	高线: 网	linux	2020-12-23 11:18:02	OED	启动 停止 卸載 删除





最近更新时间:2025-01-10 19:17:23

审计组配置可为从属于一个应用的一台或多台数据库服务器进行命名,方便后续规则配置或审计信息时,使用直观的名字来表达数据库信息,优化策略和报表可读 性。下面将为您详细介绍配置操作。

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面,详情可参见 控制台登录。

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【配置管理】>【审计组】,即可进入审计组配置页面。

#### ○ 新增审计组。

在审计组列表上方单击【添加】,在新弹出的窗口中,填写业务名,审计组名称(建议以业务应用名称为基础命名)、数据资产实例、备注信息 后,单击 【 确定】,即可新增审计组。

<ul> <li>注意</li> <li>数据库 IP 及端口必</li> </ul>	必须填写需要审计数据库的 IP 和端口,不能为0.0.0。	
添加审计组	X	
* <u>业</u> 务名:	: 如未找到相应业务,可点击这 <b>里</b> 添加	
* 审计组名称:	请输入审计组名称	
* 数据资产实例:	:	
* 备注信息:	请输入备注信息	

取消

确定

#### ○ 修改审计组。

在审计组列表中,找到需要修改的审计组,在右侧操作栏单击【修改】,在弹框中修改信息后单击【确定】即可。

修改审计组		Х
* 业务名:	→ × → → → → → → → → → → → → → → → → → →	
* 审计组名称:		
* 数据资产实例:	×	
* 备注信息:		
	取消 确:	<del>أ</del>

#### ○ 删除审计组

在审计组列表中,找到需要删除的审计组,在右侧操作栏单击【删除】,再单击询问窗中的【确定】即可。

△ 注意

删除审计组会解除该审计组下所有规则的绑定关系,如删除审计组所关联的规则仅和删除审计组有绑定关系时,该规则也会被删除。



+ 添加 ⁽¹⁾ 删除				
名称: 数据安全审计, 版本: 合规版, 最大审	計组数: 3, 已流加审计组数: 1			御除审计组金解除该审计组所所有规则的 郑定关系;如删除审计组所关联的规则仅 和删除审计组有绑定关系时,该规则也会 被删除。您确认删除所选的审计组吗?
审计组名称	包含数据库台数	部门及业务名	备注	取消 确定
test1	1	测试部-数据审计测试	0105	修改 删除



## 访问源配置

最近更新时间: 2025-01-10 19:17:23

访问源配置可为从属于同一部门或同一网络区域的访问 IP 段进行命名,方便后续规则配置、审计信息使用直观名字来表达数据库访问端信息,优化策略以及报表 可读性。下面将为您详细介绍配置操作。

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【配置管理】>【访问源】,即可进入访问源配置列表页面。

#### ○ 添加访问源

单击列表上方【添加】,在弹出窗口中,填写业务名、访问源名称、访问源包含 IP 段、备注信息,单击【确定】即可。

添加访问源			×
* 业务名:			
	如未找到相应业务,可加	点击这里添加	
•访问源名称:	请输入访问源名称		
访问源包含IP段:	起始IP	结束IP	操作
	0.0.0.1	255.255.255.254	
	增加		
*备注信息:	请输入备注信息		
			取消 确定

#### ○ 修改访问源

在访问源列表中,找到需要修改的访问源,在右侧操作栏中,单击【修改】,在弹框中修改信息后,单击【确定】即可。

			~
• <u>业</u> 务名	5:		
	如未找到相应业务,可点	击这里添加	
•访问源名利			
访问源包含IP的	2: 起始IP	结束IP	操作
	127.0.0.1	127.255.255.254	
	墙加		
* 备注信息	t: ds		
			取消 确定

#### ○ 删除访问源

在访问源列表中,找到需要删除的访问源,在右侧操作栏中,单击【删除】,再单击询问窗中的【确定】即可。

访问源名称	包含IP段数量	部门及业务名	备注	<ul> <li>您确认要删除吗?</li> </ul>
	1		ds	取消 确定
	1		ds	修改 删除



## 部门业务配置

最近更新时间: 2025-05-27 16:30:32

#### 部门业务配置包含部门配置与业务配置两大模块功能,具体配置步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中,选择【配置管理】>【部门&业务】,即可进入部门业务配置页面。

Ŀ	说明				
	如忘记登录密码,	可以	提交工单	找回密码。	

- 3. 在部门业务配置页面,可进行部门配置及业务配置。
- 部门配置
  - 3.1 在部门业务配置页面,单击【部门配置】,可添加并查看部门名、部门负责人及备注,同时可进行相关操作。

部门配置 业务配置			
+添加部门 自删除			
部门名	部门负责人	备注	操作
test	小李		修改 删除
it运营部	马忠义		修改 删除
财务部	王五		修改 删除
采购部	赵四		修改 删除

3.2 在部门设置页面,单击【添加部门】,在弹出的添加部门窗口中,填写部门名、部门负责人以及备注信息,单击【确定】即可完成添加。

添加部门	×
血口之 .	1214 \ 107747
* 部门页责人:	请输入部门负责人
备注信息:	请输入备注信息
	取消 确定

3.3 添加完成后,已添加的部门将出现在部门配置列表中,支持对已添加的部门进行修改或删除,且支持对部门信息批量选择删除。

部门曹	22 业务配置			
+ 添	加部门 自 删除			
	部门名	部门负责人	备注	操作
	test	小李		修改 删除
	it运营部	马忠义		修改 删除



○ 修改

找到需要修改的部门信息,在右侧操作栏单击【修改】,在弹出框中可以修改对应部门信息。

- 删除
- **方式1**: 找到需要删除的部门信息,在右侧操作栏单击【删除】,在弹出框中确认删除,即可完成删除。
- 方式2:选择需要删除的部门,在列表上方单击【删除】,即可批量删除部门信息。

### • 业务配置

3.1 在部门业务配置页面,单击【业务配置】,可添加并查看业务名、业务负责人、部门名及备注,同时可进行相关操作。

部门曹	部门配置业务配置						
+ 漆	加业务 自制	Â.					
	业务名	业务负责 人	部门名	备注	操作		
	test	小赵	test		修改 删除		
	薪资结算系统	meller	财务部	18	修改 删除		

3.2 在业务配置页面,单击【添加业务】,在弹出的添加业务窗口中,填写部门名、业务名、业务负责人以及备注信息,填写完成后,单击【确定】即可完成 添加。

添加业务		$\times$
*部门名:		$\sim$
* <u>业</u> 务名:	请输入业务名	
* 业务负责人:	请输入业务负责人	
备注信息:	请输入备注信息	
	取消	急定

3.3 添加完成后,已添加的业务将出现在业务配置列表中,支持对已添加的业务进行修改或删除,且支持对业务信息进行批量选择删除。

部门翻	記置 业务配置				
+ 添	前业务	\$			
	业务名	业务负责 人	部门名	备注	操作
	test	小赵	test		修改 删除
	薪资结算系统	meller	财务部	18	修改 删除

- 修改
  - 找到需要修改的业务信息,在右侧操作栏单击【修改】,在弹出框中可以修改对应业务信息。
    - 删除
      - 方式1: 找到需要删除的业务信息,在右侧操作栏单击【删除】,在弹出框中确认删除,即可完成删除。
      - **方式2**:选择需要删除的业务,在列表上方单击【删除】,在弹出框中确认删除,即可批量删除业务信息。



## 操作日志管理

最近更新时间: 2025-01-10 19:17:23

操作审计员负责审计数据安全审计各管理员的操作,防止其他管理员滥用职权进行非法操作。用操作管理员账号登录后,能够阅览管理员操作日志列表并对行为规 则进行配置。

### 日志检索

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

购	买时间	到期时间	操作
20	20-4-14	2020-5-14	管理 续费 升级

2. 以操作管理员账号登录操作日志页面,在左侧导航栏中单击**行为规则配置**,即可进入操作日志页面。

① 说明 如忘记登录率码,可以提交工单,找回率码。

3. 在操作日志页面,您可以根据操作账户、操作 IP、行为分类、操作时间检索还原非法操作完整信息。

操作日志							
操作帐户:	操作IP:	行为分类:	全部	/ 操作时间:	开始日期 ~	结束日期 📄 搜索	
			全部	<b>^</b>			
操作时间	操作	张户	登录 退出		操作IP	行为分类	操作行为
2018-05-25 11:28:36			新增配置修改配置			检索日志	检索日志
2018-05-25 11:28:35			删除配置	1		检索日志	日志检索
2018-05-25 11:28:34			导出报告	-		检索日志	日志检索

## 行为规则配置

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以操作管理员账号登录操作日志页面,在左侧导航栏中单击**行为规则配置,**即可进入行为规则配置页面。

 说明 如忘记登录密码,可以提交工单找回密码。

 在行为规则配置页面,可以查看行为操作、行为分类、告警模板、备注、是否开启告警及相关操作,同时可按照行为分类、行为操作及危险等级,对行为规则 进行搜索。





行为	分类: 全部	∨ 行为操作:	全部 🗸	危险等级: 全部	✓ 搜索		
	行为操作	行为分类	告警模版	备注	危险等级	是否开启告警	操作
	登录	用户登录	报告,有敌人来了,		低级~	开启	修改
	修改密码	用户登录			低级~	●关闭	修改

#### 字段说明:

- 行为操作:用户对系统各个账户的功能操作。
- 行为分类: 用户对系统功能操作所属的模块名
- 告警模板: 用户执行操作时邮件所发送的告警内容
- 备注:用户对行为规则的进一步说明。
- 危险等级:对用户操作行为的评级,可设置行为危险等级,包括低级、中级及高级。
- 是否开启告警:用户开启后,触发行为规则审计,则会发送告警信息,关闭后,只会记录操作,不会发送告警信息。
- ○操作:在目标行为右侧操作栏,单击**修改**,即可对行为操作信息进行修改。

修改配置		×
行为操作:	<u>登</u> 录	
行为分类:	用户登录	
接口路由:		
告警信息模板:	报告,有敌人来了,请注意,小心敌方陷阱	
备注:		
危险等级:	低级	$\sim$
是否开启告警:	●关闭	
	Į	双消 确定



## v5.0.5 系统管理 系统资源监控

最近更新时间: 2025-01-10 19:17:23

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。



2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【系统资源监控】,即可进入资源监控页面,该页面包括系统详细信息、系统存储空间统计和流量走势实时统计。



如忘记登录密码,可以 提交工单 找回密码。

#### ○ 系统详细信息

系统详细信息包含系统产品名称、系统版本等基础信息,以及数据安全审计总审计组数参数信息。

系统详情	
产品名称	and the second second
系统版本	
连续运行时长	0年0月18天13小时44分4秒
系统当前时间	2020-03-31 12:03:52
购买峰值流量	100000 QPS
已用/总审计组数	6/60个 配置Agent
自定义规则数	3个

#### ○ 系统存储空间统计

存储空间统计用于展示数据安全审计实例当前的存储状态。在系统存储空间统计右上角,单击【清理剩余空间】,将清理的数据包含所选的日期。例如, 选择了12月1日至12月3日,则会删除12月1日、2日、3日,3天的数据。

#### 🕛 说明

统计报表将磁盘空间分为四个类型:

- 剩余空间:数据安全审计实例存储剩余空间;
- 系统占用空间:数据安全审计自身代码所占存储空间;
- 审计日志占用空间: 数据安全审计记录的数据库操作信息日志占用空间;
- 其他占用空间:数据安全审计实例其他代码、配置文件占用空间。





### ○ 流量走势实时统计

流量走势实时统计能统计一定时间跨度(最近30分钟、最近24小时、最近7天)内数据安全审计中所审计的所有数据库的 QPS,确认全网 QPS 峰值是 否超过购买峰值,以帮助管理员了解数据安全审计性能状况,及时扩容升级产品。





## 用户管理

最近更新时间: 2025-05-27 16:30:32

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	ð	到期时间	操作
2020-4-1	14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中单击【用户管理】即可进入用户页面。

<b>! 说明</b> 如忘记登录	<del>!</del> 密码,可以 提交工单	找回密码。				
○ 查看账号信息 账号管理用于	-管理 DSA 实例所有则	账号。系统管理员可以	<b>山通过列表查看所有</b> 财	账号信息,包括	5所属角色、真实姓名	3、创建日期以及联系方式等 <b>。</b>
() <b>说明</b> OTP 管理员	二维码:如需开启 OT §账号下的 OTP 验证,	「P 实现登录双重验证 单击【 OTP 验证】	,可在相应账号右侧 ,查看原图并扫描起	]操作栏,单击 边态校验码。	【OTP二维码】,国	<b>找在数据安全审计管理页面右上角,找</b> 到
□ 帐号名称	所還角色 平 真实姓名 6	创建日期 创建人	最后修改人 最后修改时间	联系方式	登录19范围 操作	
sysadmin	系統管理员 2	020-09-28 10:00 系統默以创建	/ 2020-10-20 16:52	电话: 邮稿: 你怕:	研開 OTP二编码 時間	
useradmin	审计管理员 2	020-09-28 10:00 \$5:00.000 (0.000)	/ 2020-09-28 10:00	电话: 邮稿: 微信:	(平橋) (TP二條約) (平橋) (現朝)	
○ 添加账号						
如需要增加管	<b>寶理员账号,单击【添</b> 】	加账号 】,在弹框中均	真写账号信息,选择	所属角色后,鸟	自击【确定】即可。	
* 账号:						
* 密码:						
* 真实姓名:						
* 手机号码:						
* 邮箱:						
* 微信号:						
* 所属角色:	审计管理员		~			
登录IP范围:	起始IP	结束IP	操作			
	0.0.0.1	255.255.255				
	添加 (当ip为ipv6格式时,仅	对起始17有效)				

取消 确定



### ○ 修改和删除账号

如需对账号进行修改或删除,可在相应账号操作列单击【编辑】或【删除】对账号进行调整。

注意     系统默认创建账号不可删除。
----------------------

帐号名称	所還角色	Y 真实姓名	创建日期	创建人	最后核改人	最后修改时间	联系方式	登录IP范围	操作
sysadmin	系统管理员		2020-09-28 10:00	系统就认创建	T	2020-10-20 16:52	电话: 邮通: 微信:	17 (B)	OTP二编码 机5】
useradmin	市计管理员		2020-09-28 10:00	斯统默认创建	1	2020-09-28 10:00	电话: 邮稿: 网络:	17 M	OTP二维码 時間
sysaudit	操作审计管理员		2020-09-28 10:00	系统就认识能	7	2020-09-28 10:00	电话: 邮稿: 微信:	¥10	OTP二维码 调辑
-	审计管理员	-	2020-11-12 11:45	sysadmin	T	2020-11-12 11:45	电话: 1 邮编:	详细	OTP ^一 维码 编辑 删除



# Agent 管理 Agent 配置

最近更新时间: 2025-05-27 16:30:32

配置 Agent 后可将 Agent 部署在 Linux 系统或 Windows 系统,进行具体审计组配置后,实现对数据库操作的管理。

## 操作步骤

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作	
2020-4-14	2020-5-14	管理 续费	升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,选择【Agent 管理】>【Agent 配置】,即可进入 Agent 配置页面。



- 3. Agent 部署。在 Agent 配置页面,单击【配置 Agent】,可配置审计 Agent 的各类参数并提供下载链接。
- 4. 配置 Agent。配置 Agent 用于展示所有已正确安装且能实现 DSA 实例网络互通的 Agent 信息。

配置Agent				
		¥448-±15	-	8.4
审计服务时间	审计服务调出	数据库IP	审(TIP	操作F
		详情	详情	下载Linux Agent   下载Windows Agent   自删除   linux批量部署 (Windows不受持批量部署)
		详情	详情	下载Linux Agent   下载Windows Agent   ①静脉   linux批量部署 (Windows不支持批量部署)

列表各字段含义如下:

- 审计服务 IP: Agent 回传数据的源 IP。
- 审计服务端口: 该 Agent 配置的审计端口。
- 数据库 IP: 单击【详情】可查看该 Agent 审计的数据库的所有 IP 地址。
- 审计 IP:用于显示该 Agent 配置的审计范围,由于 IP 范围内容较多,可单击【详情】进行阅览。
- 操作:用于下载该 Agent 的链接。
  - 单击【下载 Linux Agent】或【下载 Windows Agent】,弹出部署 IP 窗口,可以按 IP 部署或按 IP 段部署(IP 段支持全段审计),单击【确 定】即可开始下载 Agent。

#### ▲ 注意

- 若部署机器操作系统 centos 版本号小于7.0 或者ubuntu 版本号小于11,必须勾选下方说明,否则无法部署 Agent。
- 请添加安装包需要部署机器的 IP 或 IP 列表。
- 如未添加 IP 信息却部署了会导致 Agent 无法启动。
- 如有新的机器要部署请重新下载安装包并填写机器的 IP 信息。





○ 单击【Linux 批量部署】,输入部署地址,支持按 IP 或按 IP 段部署,支持添加多行,输入服务器 IP 、SSH 端口号、用户名、密码, 输入完成 后单击【确定】即可。

部署机器操作系 ubuntu版本号小于11,	統centos版本号小于7 或者ubu 必须勾选此还项,否则无法部署age	ntu 版本号小于11 (注: ent)	艺部署机器操作系统cento	版本号小于7 3	「「「「」」
按IP部署 扬 医务器IP	SSH满口号	用户名	密码		操作
	22	root		ø	
	22	root		ø	e
加一行 : ①SSH的帐号密码服务 ②SSH第口号默认22、	3器不会保存只做下发服务使用 用户名默认root,可自行修改				



## Agent 列表

最近更新时间: 2025-01-10 19:17:23

本文将为您介绍如何查看并操作 Agent 列表。

## 操作步骤

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,选择【Agent 管理】>【Agent 列表】,即可进入 Agent 列表中。



- 3. 在 Agent 列表中,可以查看所有已配置的 Agent。Agent 列表默认展示内容包括: deployMac、部署服务器 IP、审计服务、部署状态、Agent 状态、 系统类型、部门及业务。
  - 搜索:您可以按照部署状态、Agent 状态、审计服务 IP、Port (端口)对 Agent 进行搜索。
  - 查看 Agent 配置详情:在"审计服务"栏中,单击【Agent 配置详情】,可以查看 Agent 配置相关信息。
  - 相关操作:在右侧操作栏,可以对 Agent 进行启动、停止、卸载、删除的相关操作。

Ag	jent列表							
	部署状态: 全部	×	Agent状态: 全部	V 1	审计服务 lp:		Port:	搜索
	deployMac	部署服务器IP	审计服务		部署状态	Agent状态	系统类型	部门及业务
			)(	Agent配置详情]	部署完成	正常	linux	采购部-工作服采
			ןנ	Agent配置详情]	部署完成	正常	linux	采购部-工作服采
			)[	Agent配置详情]	部署完成	正常	linux	采购部-工作服采
	4							Þ



## 时间服务器

最近更新时间: 2025-05-27 16:30:32

时间服务器主要用于同步时间,找到您需要需要同步时间的服务器IP进行设置即可,具体操作步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,在右侧操作栏,单击【管理】,进入数据安全审计登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 使用 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,单击【时间服务器】,即可进入时间服务器设置页面。

	() <b>说明</b> 如忘记登录密码,	可以 提交工单 找回密码。
3.	在时间服务器设置页面,	输入 NTP 服务器 IP,单击【提交】,即可完成设置。
	时间服务器设置	

* NTP服务器IP: 请输入NTP服务器IP

重置

4.	设置完成后,	数据安全审计系统时间会与您设置的 NTP 服务器为标准进行时间同步。	,





最近更新时间: 2025-01-10 19:17:23

告警支持针对每个审计规则策略进行告警,告警方式支持邮件告警、syslog 告警,其中系统资源告警配置可根据您设置的磁盘、内存等告警阈值,当达到阈值 时,进行告警;syslog 告警配置可配置您接收告警信息的 syslog 服务器;邮件告警配置可配置您接收告警信息的邮件服务器,具体操作步骤如下: 1. 登录 数据安全审计控制台,找到需要操作的审计系统,在右侧操作栏,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中选择【系统设置】>【告警设置】,即可进入告警设置页面。



3. 在告警设置页面,分别对告警开关、系统资源告警配置、syslog 告警配置及邮件告警配置功能进行设置。

#### ○ 告警开关

在告警设置页面,单击【告警开关】,分为【告警方式】和【告警内容】,打开需要开启告警的选项,单击【提交】,即可对 syslog 告警配置 中所设置 的服务器进行监控,且当满足告警条件时,将触发告警,并发送邮件至您所 配置的告警邮箱 中。

## ▲ 注意

若需要接收告警信息,需打开邮件告警开关,且已在邮件告警配置中设置告警接收邮箱,否则无法接收告警信息。

告警开关	系统资源告警配置	syslog告答配置	邮件告答配置	
告警方式:				
	邮件告警: 开 🔵			syslog告警: <del>开</del> )
告警内容:				
	QPS告答: 开)			sql风脸告警: 开)
	系統資源告警: 开 🔵			行为规则告警: 开
	agent掉线告警: <mark>开</mark>			
	提交			

○ 系统资源告警配置

在告警设置页面,单击【系统资源告警配置】,设置系统资源告警的触发条件,可将磁盘、内存、CPU 负载在0 - 100%之间调整,可自定义带宽值,单



#### 击【提交】,即可对 syslog 告警配置 中所设置的服务器进行监控。



#### ○ syslog 告警配置

## ⚠ 注意 目前 syslog 告警服务只支持 TCP 协议。

在告警设置页面,单击【syslog 告警配置】,输入需要记录的 syslog 服务器 IP 和端口,单击【提交】,即可完成 syslog 告警条件配置,设置完成 后接收到相关告警信息。

系统资源告答配置	syslog告警配置	邮件告警配置
* syslog服务器:		
* 端口:		
	测试 提交	注: 目前syslog告警服务只支持tcp

#### ○ 邮件告警配置

单击【邮件告警配置】,依次填入邮件服务器的相关配置信息,如需添加多个收件人,请以英文分号分隔,填写完成后,单击【提交】,当满足告警条件 时,将发送邮件至所配置的邮箱中。

⚠	注意	
	若填写 QQ 邮箱账号,	密码需填写所设置的邮箱密码。



告警开关	系统资源告誓配置 syslog告誓配置 邮件告誓配置
* SMTP服务器	
UTTER AND AND	第三方邮件服务容易受服务器反垃圾机制影响,如遇到不可用的, 建议尝试切换其他邮件服务
* 端口	
* 邮件账号	:
* 密码	
* 发件人	
收件人	:
122	多个收件人请以分号;分隔 · Z
555	
	测试 提交 里直



## 备份服务器

最近更新时间: 2025-01-10 19:17:23

为了您审计数据的安全,我们为您提供了备份服务器设置,当设置了具体的服务器地址、路径等项目后,将按天备份审计数据。

≙	· 注意		
	建议您在配置好数据审计服务后,	第一时间设置备份服务器,	达到审计数据的及时安全备份。

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作		
2020-4-14	2020-5-14	管理	续费	升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,选择【系统设置】>【备份服务器设置】,即可进入备份服务器设置页面。



在备份服务器设置页面,依次输入备份服务器地址、备份服务器端口、备份服务器用户名、备份服务器密码、备份服务器目录路径,打开备份开关,单击【保存】即可完成备份服务器设置。

备份服务器设置	
备份服务器地址:	
备份服务器端口:	22
备份服务器用户名:	root
备份服务器密码:	
备份服务器目录路径	/data/beifen
备份开关:	Ħ
[	保存

4. 设置完成后,数据安全审计管理系统中的数据将会按照设置路径进行备份。



## OTP 设置

最近更新时间: 2025-05-27 16:30:32

本文档将为您介绍如何开启 OTP 校验,并通过 OTP 校验登录数据安全审计管理页面。

## 操作步骤

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以 sysadmin 账号登录数据安全审计管理页面,在左侧导航栏中,选择【系统设置】>【OTP 设置】,即可进入 OTP 设置页面。



3. 在 OTP 设置页面,设置校验开关,如需开启 OTP 验证选项,选中开启 OTP 验证,单击【保存】,退出登录系统即可。

|--|

OTP设置		
	校验开关: ● 开启OTP验证 ○ 关闭OTP验证	
	保存	

4. 再次登录数据安全审计管理页面,需要输入OTP 校验码。





## 审计管理 审计数据

最近更新时间: 2025-05-27 16:30:32

### 审计概览

- 1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面,详情可参见 控制台登录 。
- 2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【审计数据】>【审计概览】,即可进入审计概览页面。
- 在审计概览页面中,可总览全网数据库各类排行信息以及查询单个数据库实例概览信息,如需了解数据库审计组详细内容,可在审计概览页面下方查询审计组 的详细信息。
  - 数据库排行统计:上方条形统计图为数据库排行,排行统计数据内容如下:
    - 风险排行:用于统计全网各数据库风险总数,降序排列。
    - 语句压力排行:用于统计全网各数据库语句压力总数,降序排列。
  - 审计组详情:审计组详情内可查看您所配置的审计组的风险分布 Top5、语句压力统计 Top5(QPS),会话分布 Top5,还可按照全部、高风险、中风 险、低风险进行查看各个风险级别详细数据,每个报表可展示三种走势图及三类风险级别数据:
    - 风险分布:用于展示本数据库审计组高中低三类风险的统计信息,展示时间范围可在1天到365天之间进行调整。
    - 自定义规则命中:用于展示与本数据库审计组有关的自定义规则命中信息,展示时间范围可在1天到365天之间进行调整。
    - 语句压力统计:用于展示本数据库审计组语句压力的统计信息,展示时间范围可在1天到365天之间进行调整。
    - 会话统计:用于展示本数据库审计组各类会话信息,展示时间范围可在1天到365天之间进行调整。

~				天 7天 30天 90天 6个月 1年
-0- 审计员工系统 -0-	审计座机系统 -○- 审计签列系统 -<	(金幣) ? ○- 审计工作服系购系统		
and sold I have not a serie	ald the second sec			
06:00 04-02	12:00 04-02	18:00 04-02	23:59 04-02	
	12 ¹ 03	18:00	2299	
Q- 新计员工系统 -Q- 新计控机系统	f -O- 非计进到系统 -O- 非计工作	● 新田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田	ea (200-ea (200-ea)	
06-02 06-02	12:00 04-02	18:00 04-02	23:59 04-02	

## 日志检索

日志检索主要提供日志查询与导出功能。

- 1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面,详情可参见 控制台登录。
- 2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【审计数据】>【日志检索】,即可进入日志检索页面。



#### 3. 管理员通过 审计概览 定位到疑似有风险的数据库审计组,或者企业网络已经发生数据库安全问题时,可在日志检索页面查询并导出日志信息。

审计组: 审计员工系统× 审计签到系统× 审计工作服采购系统× 审计座机系统× 审计薪资结算系统× 审计网络管理系统×

风险等级:	全部		名: 请输入	命中	親则: 无	V		查询 导出 展开∨
最近一小	最近一小时 今天 昨天 本周 上周 本月 上月 自定义							
	✓ 查询已完成, 数据总量: 37,376,883 条							
序号	数据库用户	客户端IP	时间	命中规则	访问源	审计组名	风险等级	SQL语句
1	0.00	1710 10288 8.	04-13 11:07:43		11000	审计员工	• 正常	login_err
2		1.71.1.21.00.000	04-13 10:59:33		11000	审计工作	• 正常	login_err

### 日志查询

在日志检索页面,您可以按照审计组、风险等级、用户名、命中规则及时间,对日志进行查询。

审计组:	审计员工系统×	审计签到系统×	审计工作服采购系统 X	审计座机系统X	审计薪资结算系统X	审计网络管理器	系统 X		
风险等级	全部		∨ 用户名: 请	俞入		命中规则: 无		查询	导出 展开∨
最近一	小时今天『	F 本周 上	周本月上月	自定义					

### 查看数据详情

在日志列表中,可单击某条记录查看其详细内容。

1 第1条数据详情	
SQL语句:	
SQL类型:	SelectStmt
操作时间:	05-23 21:40
SessionID :	
命中规则:	AI-高风险,1
风险等级:	<ul> <li>高风险</li> </ul>
数据库:	
数据库IP:	
数据库用户:	root
表名:	
影响行数:	10
执行时间:	0
返回消息:	
返回码:	0
实例ID:	
客户端IP:	

## 日志导出

检索出需要导出的数据,现已支持不限数量导出,在列表上方单击【导出】,弹出导出数据弹窗,单击【确定】即可将数据导出,导出文件类型为 Excel ( .xlsx格式 )。





## 审计配置 审计组配置

最近更新时间:2025-01-10 19:17:23

审计组配置可为从属于一个应用的一台或多台数据库服务器进行命名,方便后续规则配置或审计信息时,使用直观的名字来表达数据库信息,优化策略和报表可读 性,下面将为您详细介绍配置操作。

### 操作步骤

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面,详情可参见 控制台登录 。

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【审计配置】>【审计组配置】,即可进入审计组配置页面。

#### ○ 新增审计组。

在审计组列表上方单击【添加】,在新弹出的窗口中,填写业务名,审计组名称(建议以业务应用名称为基础命名)、数据库类型、数据库 IP、数据库端 口、版本信息、备注信息后,单击【确定】即可新增审计组。

## ① 注意

数据库 IP 及端口必须填写需要审计数据库的 IP 和端口,不能为0.0.0.0。

添加审计组				Х
<ul> <li>业务名:</li> </ul>				
	如未找到相应业务,可	「点击这里源加		
• 审计组名称:	请输入审计组名称			
数据库类型:	Mysql 5.1-5.7			×
数据库:	数据库IP	数据库端口	操作	
	以访问本地数据库为例	),须配置ip:127.0.0.1, port	3306(mysql默认嫡囗为3306	)
	0.0.0.0	3306		
	増加 山 文件批量导	λ		
	批量导入的文件格式为		11.23.10:3306)	
<ul> <li>备注信息:</li> </ul>	请输入备注信息			

#### ○ 修改审计组。

在审计组列表中,找到需要修改的审计组,在右侧操作栏单击【修改】,在弹框中修改信息后单击【确定】即可。

	如未找到相应业务,可点;	<u> </u>		
• 审计组名称:				
数据库类型:	Mysql 5.1-5.7			
数据库:	数据库IP	数据库端口	操作	
	以访问本地数据库为例, 《 增加 上 文件批量导入 批量导入的文件格式为每/	页配置ip:127.0.0.1, por	:3306(mysqા默认端口为330 .11.23.10:3306)	16)
• 备注信息:	dsa			

#### ○ 删除审计组

在审计组列表中,找到需要删除的审计组,在右侧操作栏单击【删除】,再单击询问窗中的【确定】即可。



审计组名称	包含数据库台数	部门及业务名	备注	操作
	1	1 m 1 m 1	dsa	0 您确认要删除吗?
	1		das	取消 确定
	1		dsa	修改删除

▲ 注意

删除审计组会解除该审计组下所有规则的绑定关系,如删除审计组所关联的规则仅和删除审计组有绑定关系时,该规则也会被删除。

+ 添加 ① 删除				
名称: 数据安全审计, 版本: 合规版, 最大审	计组数: 3, 已添加审计组数: 1			創除审计组会解除该审计组下所有规则的 规定关系;如删除审计组下关系的规则仅 和删除审计组有规定关系时,该规则也会 增需则除审计组同的ECEPATC中计增加2
<b>审计组</b> 名称	包含数据库台数	部门及业务名	备注	10回94. 2046A回9477233年11日号? 取消 <mark>确定</mark>
test1	1	测试部-数据审计测试	0105	修改 删除



## 访问源配置

最近更新时间: 2025-01-10 19:17:23

访问源配置可为从属于同一部门或同一网络区域的访问 IP 段进行命名,方便后续规则配置、审计信息使用直观名字来表达数据库访问端信息,优化策略以及报表 可读性。下面将为您详细介绍配置操作。

### 操作步骤

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中单击【审计配置】>【访问源配置】即可进入访问源配置列表页面。

① <b>说明</b> 如忘记登录密码,可以 提交工单 找回密码。

单击列表上方【添加】,在弹出窗口中,填写业务名、访问源名称、访问源包含 IP 段、备注信息,单击【确定】即可。

找到相应业务,可点击	日这里添加	
喻入访问源名称		
IP	结束IP	操作
.0.1	255.255.255.254	
扇入备注信息		
		取消 确定
	线到相应业务,可点面 最入访问原名称   <b>P</b> .0.1 最入备注信息	成到相应业务,可点击这里添加 最入访问源名称 IP .0.1 全支5.255.255.254 自入留注信息

#### ○ 修改访问源

在访问源列表中,找到需要修改的访问源,在右侧操作栏中,单击【修改】,在弹框中修改信息后,单击【确定】即可。

修改访问源			×
• 业务名:	如未找到相应业务,可点	击 <u>这舉</u> 添加	
•访问源名称:			
访问源包含IP段:	起始IP	结束IP	操作
	127.0.0.1	127.255.255.254	
	增加		
* 备注信息:	ds		
			取消 确定

#### ○ 删除访问源

在访问源列表中,找到需要删除的访问源,在右侧操作栏中,单击【删除】,再单击询问窗中的【确定】即可。



访问源名称	包含IP段数量	部门及业务名	备注	您确认要删除吗?
	1		ds	取消 确定
	1		ds	修改删除



## 规则配置

最近更新时间: 2025-05-27 16:30:32

规则配置可定义数据安全审计的审计组的安全规则。数据安全审计具备两个默认规则,AI 引擎规则和 CVE 引擎规则,默认规则不可删除、不可编辑,下面将为 您详细介绍配置操作。

### 操作步骤

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

Ŗ	9买时间	到期时间	操作
2	020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中,选择【审计配置】>【规则配置】,即可进入规则配置页面。

#### 新建规则

如需自定义规则满足个性化审计需求,单击【添加规则】,进入新建规则页面,填写规则名称等,单击【保存】即可。

### △ 注意

- 规则配置支持同一规则配置多个条件,多个条件之间为"与"关系,必须全部匹配才能够触发规则和告警。
- 自定义规则默认为黑名单,触发后将产生告警并且记录入库。如果管理员需要节省数据安全审计的审计组的存储空间,指定部分操作行为不记录不入 库,可在规则中指定相关操作后,选择"白名单"选项,并且将告警选项都取消。

以上操作完成后,即可实现白名单类型规则配置,减少误报、减轻数据安全审计的审计组存储压力。

规则类型:	● 黑名单 ○ 白名単				
* 规则名称:	请输入规则名称				
	不超过15个中文字符长度	,支持中文、英文以及			
涉及审计组:	请选择审计组				
规则备注:	选填				
条件设置:	字段	条件	值	操作	
	×	×			
	请选择字段名称				
	添加				
危险等级:	低风险				$\vee$
告警:					

#### • 规则示例

在规则配置页面,单击【添加规则】,按下图配置规则,表名和阈值根据您的业务场景自行设定,单击【保存】即可。



」名称:	请输入规则名称				
	不超过15个中文字符长度,支持中	中文、英文以及			
计组:	请选择审计组				
F注:	选填				
设置:	字段	条件	値	操作	
	表名(tb_name) V	包含	∨ xxx_test		
	SQL类型(sql_type) V	包含	<ul> <li>✓ select</li> </ul>	#SPA:	
	影响行数(effect_row) 🛛 🗸	大于等于	× 50	删除	
	添加				
- 692 493 -	任风险				

### • 规则配置建议

以下三个建议规则仅作为示例,用户可根据自身业务自行配置。

○ 防爬取规则:防止使用例如 select 操作语句,爬取表数据。

规则类型: ● 黑名单 ● 白名单 • 规则名称: 防疤取策略 不超过15个中文字符长度,支持中文、英文以及 涉及审计相: test × 规则备注: 选项 条件 值 操作 ⑤L送型(sql_type) ∨ 包含 ∨ select ■ 影响行致(effect_row) ∨ 大于等于 ∨ 100 删除 添加 危险等极: 低风险	<u>小</u> 注 影	意 响行数可以根据业务自行配	置。		
<ul> <li>*规则名称: 防爬取策略         不超过15个中文字符长度,支持中文、英文以及     </li> <li>涉及审计相: test ×         规则备注: 选填         您有         值 操作         值 操作         ⑤QL类型(sqLtype) ∨ 包含 ∨ select         》 例前行数(effect_row) ∨ 大子等于 ∨ 100 删除         派加         危险等级: 低风险         告答: □     </li> </ul>	规则类型:	<ul> <li>黑名单</li> <li>白名单</li> </ul>			
不超过15个中文字符长度,支持中文、英文以及         涉及审计组:         建工         規则备注:       透照         条件设置:       字段       条件       值       操作         ⑤(L类型(sql_type))        包含       ✓       select       原始         序加                唐鑒:	•规则名称:	防爬取策略			
沙及审计组: test ×  规则备注: 透填		不超过15个中文字符长度,支持中文、	英文以及		
規则备注: 透填 条件设置: 字段 条件 值 操作 SQL类型(sqLtype) ∨ 但含 ∨ select 影响行数(effect_row) ∨ 大于等于 ∨ 100 删除 添加 た脸等级: 低风险	涉及审计组:	test ×			
条件设置:字段     条件     值     操作       SQL类型(sql_type)       select       影响行数(effect_row)      大于等于     100        添加          吉蓉:	规则备注:	选填			
SQL类型(sql_type)        select       影响行数(effect_row)       大于等于      100        添加             危险等级:     低风险	条件设置:	字段	条件	值	操作
影响行数(effect_row)        添加       危险等级:       伍风险		SQL类型(sql_type) V	<b>包含</b>	select	
添加 危险等级: 低风险 音警: □		影响行数(effect_row) V	大于等于 🗸	100	删除
危险等级: 任风险 告答: □		添加			
告答:	危险等级:	低风险			
	告答:				
保存取消		保存取消			

执行时间可以根据业务自行配置。



规则名称:	请输入规则名称					
	不超过15个中文字符长度,支持中文、英	文以及				
》及审计组:	请选择审计组					
规则备注:	选填					
规则备注: 条件设置:	选填 字段 操作类型(sql_type)	V	<b>条件</b> 包含	V	<b>伯</b> select	操作
规则备注: 条件设置:	选项 <b>学段</b> 操作类型(iqi_type) 执行音词(exec_time)	v 	<b>条件</b> 包合 大于等于	v v	值 select 500.00 毫秒	操作
规则备注: 条件设置:	透頻 学段 操作类型(sql_type) 执行时间(exec_time) 添加	v v	<u>条件</u> 包含 大于等于	× ] × ]	值 select 500.00 毫秒	操作

○ 危险操作规则:检查执行 DELETE/DROP/ALTER 等类型的高危 SQL 语句。

▶ 规则名称:								
	下超过15个中文字符长度,支持中文、英文以及							
涉及审计组:	test ×	test ×						
规则备注:	选项							
条件设置:	字段	条件	值	操作				
	SQL类型(sql_type)	/ 包含	∨ drop					
	添加							
危险等级:	低风险							
告惑								

### 修改规则

在规则列表中,找到需要修改的规则,在右侧操作栏中,单击【修改】,修改信息后单击【保存】即可。

-			修改 删除
CVE引擎	全部	系统内置规则	修改
AI引擎	全部	系统内置规则	修改
规则名称	涉及审计组	衛注	操作

## 删除规则

在规则列表中,找到需要删除的规则,在右侧操作栏中,单击【删除】,再单击询问窗【确定】即可。

	<ul> <li>您确认要删除吗?</li> <li>取消</li> <li>確定</li> </ul>
	修改 删除



## 部门业务配置

最近更新时间: 2025-01-10 19:17:23

#### 部门业务配置功能主要是部门配置与业务配置的相关功能,具体配置步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中,选择【配置管理】>【部门&业务】,即可进入部门业务配置页面。

1	说明				
	如忘记登录密码,	可以	提交工单	找回密码。	

- 3. 在部门业务配置页面,可进行部门配置及业务配置。
- 部门配置
  - 3.1 在部门业务配置页面,单击【部门配置】,可添加并查看部门名、部门负责人及备注,同时可进行相关操作。

部门配置 业务配置			
+ 添加部门 日 删除			
部门名	部门负责人	备注	操作
test	小李		修改 删除
it运营部	马忠义		修改 删除
□ 财务部	王五		修改 删除
采购部	赵四		修改 删除

3.2 在部门设置页面,单击【添加部门】,在弹出的添加部门窗口中,填写部门名、部门负责人以及备注信息,单击【确定】即可完成添加。

添加部门	×
. 如门夕.	1246 \ 47/7-F
* 라이 나는 :	「「「「「」」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」、「」、」、「」、
★部门负责人:	请输入部门负责人
备注信息:	请输入备注信息
	取消 确定

3.3 添加完成后,已添加的部门将出现在部门配置列表中,支持对已添加的部门进行修改或删除,且支持对部门信息批量选择删除。

部门曹	記置 业务配置			
+ 添	加部门 ① 删除			
	部门名	部门负责人	备注	操作
	test	小李		修改 删除
	it运营部	马忠义		修改 删除



○ 修改

找到需要修改的部门信息,在右侧操作栏单击【修改】,在弹出框中可以修改对应部门信息。

- 删除
- **方式1**: 找到需要删除的部门信息,在右侧操作栏单击【删除】,在弹出框中确认删除,即可完成删除。
- 方式2:选择需要删除的部门,在列表上方单击【删除】,即可批量删除部门信息。

### • 业务配置

3.1 在部门业务配置页面,单击【业务配置】,可添加并查看业务名、业务负责人、部门名及备注,同时可进行相关操作。

部门酉	記置 业务配置				
+ 漆	加业务 ① 删	<b>☆</b>			
	业务名	业务负责 人	部门名	备注	操作
	test	小赵	test		修改 删除
	薪资结算系统	meller	财务部	18	修改 删除

3.2 在业务配置页面,单击【添加业务】,在弹出的添加业务窗口中,填写部门名、业务名、业务负责人以及备注信息,填写完成后,单击【确定】即可完成 添加。

添加业务		$\times$
*部门名:		$\sim$
* <u>业</u> 务名:	请输入业务名	
* 业务负责人:	请输入业务负责人	
备注信息:	请输入备注信息	
	取消	确定

3.3 添加完成后,已添加的业务将出现在业务配置列表中,支持对已添加的业务进行修改或删除,且支持对业务信息进行批量选择删除。

部门酉	记置 业务配置				
+ 漆	加业务 🗋 刑师	<b>æ</b>			
	业务名	业务负责 人	部门名	备注	操作
	test	小赵	test		修改 删除
	薪资结算系统	meller	财务部	18	修改 删除

- 修改
  - 找到需要修改的业务信息,在右侧操作栏单击【修改】,在弹出框中可以修改对应业务信息。
    - 删除
      - 方式1: 找到需要删除的业务信息,在右侧操作栏单击【删除】,在弹出框中确认删除,即可完成删除。
      - **方式2**:选择需要删除的业务,在列表上方单击【删除】,在弹出框中确认删除,即可批量删除业务信息。



## 自定义报表

最近更新时间: 2025-01-10 19:17:23

自定义列表功能主要展示所有配置过的审计组数据,并提供搜索、导出及 PDF 下载功能,具体操作步骤如下:

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击【管理】,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以审计管理员账号登录数据安全审计管理页面,在左侧导航栏中选择【报表】>【自定义报表】,即可进入自定义报表页面。

## 说明 如忘记登录密码,可以提交工单找回密码。

3. 在自定义报表页面中,可查看内容包括报告名称、报告说明及发送目标等字段,同时可以进行相关操作,每个页面默认展示10条数据,可按照报告名称、生成 方式、开始时间及结束时间,对报告进行搜索,还可下载 PDF 报告。

◎ 定时生成报表 Ш	即时生成报表						
报告名称:	生成方式: 全部	∨ 开始时间: 请	选择日期 芭	结束时间:	请选择日期	<b>尚</b> 搜	宏
报告名称	报告说明	发送目标	报告生成时间	生成方式	状态	操作	
定时_2020-04-20	测试定时day1911	sysadmin	04-20 19:11	定时生成	已生成	查看 pdf下载	删除
定时_2020-04-20	测试定时month	sysadmin	04-20 16:10	定时生成	已生成	查看   pdf下载	一删除

### • 定时生成报表

数据安全审计管理系统支持定时生成报表,在报表上方单击【定时生成报表】,弹出定时生成报表弹窗,依次输入模板名称、统计周期(可选择定时执行、每 天一次、每周一次、每月一次)、执行时间(精确到时分秒)、报告说明,设置完成后,单击【确定】,即可在您设定的执行时间定时生成报表。

定时生成报	表	×
* 模板名称:	审计日报 最多30个字符	
统计周期:	每天—次 🗸	
* 执行时间:	02:00:00 ① 注:建议导出时间为凌 晨1点	
* 报告说明:	dsa	
	最多200个字符	
	取消	确定

#### • 即时生成报表

数据安全审计管理系统支持即时生成报表,即生成某个时间段内的报表,单击【即时生成报表】,依次输入报告名称、统计开始时间、统计结束时间、报告说 明,单击【确定】,即可输出您规定的时间范围内的报表。

▲ 注意		
开始时间应早于结束时间。		



即时生成报表		×
* 报告名称:	最多30个字符	
* 统计开始时间:	2020-04-12 00:00:00	Ë
* 统计结束时间:	2020-04-12 23:59:59	Ë
* 报告说明:		1
	最多200个字符	
		取消 确定



## 操作日志管理

最近更新时间: 2025-01-10 19:17:23

操作审计员负责审计数据安全审计各管理员的操作,防止其他管理员滥用职权进行非法操作。用操作管理员账号登录后,能够阅览管理员操作日志列表并对行为规 则进行配置。

### 日志检索

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

购买时间	到期时间	操作
2020-4-14	2020-5-14	管理 续费 升级

2. 以操作管理员账号登录操作日志页面,在左侧导航栏中单击**行为规则配置**,即可进入操作日志页面。

()	说明
	如忘记登录密码,可以 提交工单 找回密码。

3. 在操作日志页面,您可以根据操作账户、操作 IP、行为分类、操作时间检索还原非法操作完整信息。

操作E	志											
操作	帐户:	操作IP:	f.	亏为分类:	全部	^	操作时间:	开始日期	~ 结	束日期	││────────────────────────────────────	
					全部	-						
操	作时间		操作账户		登录 退出	ł		操作IP			行为分类	操作行为
20	18-05-25 11:28:36				新增配置 修改配置						检索日志	检索日志
20	18-05-25 11:28:35				删除配置 检索日本	ł					检索日志	日志检索
20	18-05-25 11:28:34				导出报告	•					检索日志	日志检索

## 行为规则配置

进行搜索。

1. 登录 数据安全审计控制台,找到需要操作的审计系统,单击管理,进入数据安全审计管理系统登录界面。

审计系统实例名	IP地址	已购规格	购买时间	操作
	公网IP: 内网IP:	合规版	2018-5-23	管理
购买时间	到期时间	操作		
2020-4-14	2020-5-14	管理 续费 升级		

2. 以操作管理员账号登录操作日志页面,在左侧导航栏中单击**行为规则配置**,即可进入行为规则配置页面。

	<ul> <li><b>说明</b></li> <li>如忘记登录密码</li> </ul>	h,可以 提交工单 找	回密码。						
3.	在行为规则配置页面,	可以查看行为操作、	行为分类、	告警模板、	备注、	是否开启告警及相关操作,	同时可按照行为分类、	行为操作及危险等级,	对行为规则

① 说明

所有数据由系统内建生成,用户可以根据需求进行修改。



行为分类: 全部	∨ 行为操作:	全部	∨ 危险等级: 全部	∨捜索		
行为操作	行为分类	告警模版	备注	危险等级	是否开启告警	操作
登录	用户登录	报告, 有敌人来了	7,	低级>	开启	修改
修改密码	用户登录			低级>	(关闭	修改

#### 字段说明:

- 行为操作:用户对系统各个账户的功能操作。
- 行为分类: 用户对系统功能操作所属的模块名
- 告警模板:用户执行操作时邮件所发送的告警内容。
- 备注: 用户对行为规则的进一步说明。
- 危险等级:对用户操作行为的评级,可设置行为危险等级,包括低级、中级及高级。
- 是否开启告警:用户开启后,触发行为规则审计,则会发送告警信息,关闭后,只会记录操作,不会发送告警信息。
- ○操作:在目标行为右侧操作栏,单击修改,即可对行为操作信息进行修改。

修改配置	2	K
行为操作:	<u>登</u> 录	
行为分类:	用户登录	
接口路由:		
告警信息模板:	报告,有敌人来了,请注意,小心敌方陷阱	
备注:		ĺ
危险等级:	低级 ~	2 
是否开启告警:		
		_
	取消 确定	