ALIBABA CLOUD

阿里云

云安全中心（态势感知）

调查响应

文档版本：20220711

阿里云

法律声明

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

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

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

目录

1.日志详细字段说明

本文档提供了云安全中心日志的字段说明。

实时数据

字段名	说明	示例
dir	网络连接方向。取值： • in：入方向 • out：出方向	in
src_ip	网络连接发起者的IP。 • dir为out时表示本机 • dir为in时表示对端主机	10.240.XX.XX
src_port	网络连接发起者的端口。	24680
dst_ip	网络连接接收者的IP。 • dir为out时表示对端主机 • dir为in时表示本机	10.240.XX.XX
dst_port	网络连接接收者端口。	22
status	网络连接状态。 说明 实时日志中该参数的取值为随机赋予，取值无任何意义，您无需关注。	2
type	实时网络连接的类型。取值： • connect：主动发起TCP connect连接 • accept：收到TCP连接 • listen：端口监听	listen

快照数据（资产指纹）

字段名	说明	示例
proc_path	进程路径。	"/usr/sbin/sshd"
proc_cmdline	进程命令行。	"/usr/sbin/sshd -D"
pid	进程ID。	1158
ppid	父进程ID。	1

字段名	说明	示例
dir	网络连接方向。取值： • in：入方向 • out：出方向	in
src_ip	网络连接发起者的IP。 • dir为out时表示本机 • dir为in时表示对端主机	10.240.XX.XX
src_port	网络连接发起者的端口。	24680
dst_ip	网络连接接收者的IP。 • dir为out时表示对端主机 • dir为in时表示本机	10.240.XX.XX
dst_port	网络连接接收者端口。	22
status	网络连接状态。取值： • 1：TCP_STATE_CLOSED（连接关闭/未打开） • 2：TCP_STATE_LISTEN（监听中） • 3：TCP_STATE_SYN_SENT（发送SYN包） • 4：TCP_STATE_SYN_RCVD（SYN包已接收） • 5：TCP_STATE_ESTABLISHED（已建立连接） • 6：TCP_STATE_CLOSE_WAIT（等待关闭） • 7：TCP_STATE_CLOSING（双方都在关闭连接） • 8：TCP_STATE_FIN_WAIT1（主动关闭方发送FIN等待ACK） • 9：TCP_STATE_FIN_WAIT2（主动关闭方收到ACK） • 10：TCP_STATE_LAST_ACK（被动关闭方等待ACK） • 11：TCP_STATE_TIME_WAIT（主动关闭方收到FIN并发送ACK）	2

网络日志

DNS解析日志

字段名	说明	示例
additional	additional字段，竖线分隔。	无
additional_num	additional字段数量。	0
answer	DNS回答信息，竖线分隔。	example.com A IN 52 1.2.XX.XX
answer_num	DNS回答信息数量。	1
authority	authority字段。	NS IN 17597
authority_num	authority字段数量。	1
client_subnet	客户端子网。	172.168.XX.XX
dst_ip	目标IP。	1.2.XX.XX
dst_port	目标端口。	53
in_out	数据的传输方向，取值： • **in**：流入 • **out**：流出	out
qid	查询ID。	12345
qname	查询域名。	example.com
qtype	查询类型。	A
query_datetime	查询时间戳（毫秒）。	1537840756263
rcode	返回代码。	0
region	来源区域ID。取值： • 1：北京 • 2：青岛 • 3：杭州 • 4：上海 • 5：深圳 • 6：其他	1
response_datetime	返回时间。	2018-09-25 09:59:16
src_ip	源IP地址。	1.2.XX.XX
src_port	源端口。	22

本地DNS日志

字段名	说明	示例
answer_rda	DNS回答信息，竖线分隔。	example.com
answer_ttl	DNS回答的时间周期，竖线分隔。	100
answer_type	DNS回答的类型，竖线分隔。	1
anwser_name	DNS回答的名称，竖线分隔。	example.com
dest_ip	目标IP地址。	1.2.XX.XX
dest_port	目标端口。	53
group_id	分组ID。	3
hostname	主机名。	hostname
id	查询的ID。	64588
instance_id	实例ID。	i-2zeg4zldn8zypsfg****
internet_ip	公网IP地址。	1.2.XX.XX
ip_ttl	IP的周期。	64
query_name	查询的域名。	example.com
query_type	查询的类型。	A
src_ip	源IP地址。	1.2.XX.XX
src_port	源端口。	1234
time	查询时间戳（秒）。	1537840756
time_usecond	响应耗时（微秒）。	49069
tunnel_id	通道ID。	514763

网络会话日志

字段名	说明	示例
asset_type	产生日志的资产。取值： • ECS • SLB • RDS	ECS
dst_ip	目标IP地址。	1.2.XX.XX

字段名	说明	示例
dst_port	目标端口。	53
proto	协议类型。取值： • tcp • udp	tcp
session_time	会话开始时间。	2018-09-25 09:59:49
src_ip	源IP地址。	1.2.XX.XX
src_port	源端口。	54

Web访问日志

字段名	说明	示例
content_length	消息实体的传输长度。单位为：字节。	123
dst_ip	目的IP地址。	1.2.XX.XX
dst_port	目的端口。	54
host	访问的主机。	47.XX.XX.158:8080
jump_location	重定向地址。	123
method	HTTP请求方式。	GET
referer	客户端向服务器发送请求时的HTTP referer，告知服务器访问来源的HTTP连接。	www.example.com
request_datetime	请求时间。	2018-09-25 09:58:37
ret_code	返回状态值。	200
rqs_content_type	请求内容类型。	text/plain;charset=utf-8
rsp_content_type	响应内容类型。	text/plain; charset=utf-8
src_ip	源IP地址。	1.2.XX.XX
src_port	源端口。	54
uri	请求URI。	/report
user_agent	向用户客户端发起的请求。	okhttp/3.2.0

字段名	说明	示例
x_forward_for	路由跳转信息。	1.2.XX.XX

安全日志

漏洞日志

字段名	说明	示例
name	漏洞名称。	oval:com.redhat.rhsa:def:20182390
alias_name	漏洞别名。	RHSA-2018:2390: kernel security and bug fix update
op	漏洞的处理动作。取值： • new：新增 • verify：验证 • fix：修复	new
status	漏洞状态信息。	1
tag	漏洞的标签。取值： • oval：Linux软件漏洞 • system：Windows系统漏洞 • cms：Web-CMS漏洞 说明 其他类型的漏洞的标签为随机字符串。	oval
type	漏洞类型。取值： • sys：windows系统漏洞 • cve：Linux软件漏洞 • cms：Web-CMS漏洞 • emg：紧急漏洞	sys
uuid	服务器UUID。	1234-b7ca-4a0a-9267-12****

基线日志

字段名	说明	示例
level	风险项级别。取值： • high：高 • mediam：中 • low：低	low

字段名	说明	示例
op	操作信息。取值： • new：新增 • verity：验证	new
risk_name	风险项名称。	密码策略合规检测
status	状态信息。更多信息，请参见安全日志状态码。	1
sub_type_alias	子类型别名（中文）。	系统账户安全
sub_type_name	子类型名称。	system_account_security
type_name	检测类型名称。	account
type_alias	类型别名（中文）。	cis
uuid	检测出当前风险项的服务器UUID。	12345-b7ca-4a0a-9267-123456

基线类型及子类型列表

类型名称	子类型名称	描述
hc_exploit	hc_exploit_redis	高危风险利用-Redis未授权访问高危风险
hc_exploit	hc_exploit_activemq	高危风险利用-ActiveMQ未授权访问高危风险
hc_exploit	hc_exploit_couchdb	高危风险利用-CouchDB未授权访问高危风险
hc_exploit	hc_exploit_docker	高危风险利用-Docker未授权访问高危风险
hc_exploit	hc_exploit_es	高危风险利用-Elasticsearch未授权访问高危风险
hc_exploit	hc_exploit_hadoop	高危风险利用-Hadoop未授权访问高危风险
hc_exploit	hc_exploit_jboss	高危风险利用-Jboss未授权访问高危风险
hc_exploit	hc_exploit_jenkins	高危风险利用-Jenkins未授权访问高危风险
hc_exploit	hc_exploit_k8s_api	高危风险利用Kubernetes-Apiserver未授权访问高危风险
hc_exploit	hc_exploit_ldap	高危风险利用-LDAP未授权访问高危风险（Windows环境）
hc_exploit	hc_exploit_ldap_linux	高危风险利用-openLDAP未授权访问高危风险（Linux环境）
hc_exploit	hc_exploit_memcache	高危风险利用-Memcached未授权访问高危风险

类型名称	子类型名称	描述
hc_exploit	hc_exploit_mongo	高危风险利用-Mongodb未授权访问高危风险
hc_exploit	hc_exploit_pgsql	高危风险利用-Postgresql未授权访问高危风险基线
hc_exploit	hc_exploit_rabbitmq	高危风险利用-RabbitMQ未授权访问高危风险
hc_exploit	hc_exploit_rsync	高危风险利用-rsync未授权访问高危风险
hc_exploit	hc_exploit_tomcat	高危风险利用-Apache Tomcat AJP文件包含漏洞风险
hc_exploit	hc_exploit_zookeeper	高危风险利用-ZooKeeper未授权访问高危风险
hc_container	hc_docker	阿里云标准-Docker安全基线检查
hc_container	hc_middleware_ack_master	CIS标准-Kubernetes(ACK) Master节点安全基线检查
hc_container	hc_middleware_ack_node	CIS标准-Kubernetes(ACK) Node节点安全基线检查
hc_container	hc_middleware_k8s	阿里云标准-Kubernetes-Master安全基线检查
hc_container	hc_middleware_k8s_node	阿里云标准-Kubernetes-Node安全基线检查
cis	hc_suse 15_djbh	等保三级-SUSE 15合规基线检查
cis	hc_aliyun_linux3_djbh_l3	等保三级-Alibaba Cloud Linux 3合规基线检查
cis	hc_aliyun_linux_djbh_l3	等保三级-Alibaba Cloud Linux/Aliyun Linux 2合规基线检查
cis	hc_bind_djbh	等保三级-Bind合规基线检查
cis	hc_centos 6_djbh_l3	等保三级-CentOS Linux 6合规基线检查
cis	hc_centos 7_djbh_l3	等保三级-CentOS Linux 7合规基线检查
cis	hc_centos 8_djbh_l3	等保三级-CentOS Linux 8合规基线检查
cis	hc_debian_djbh_l3	等保三级-Debian Linux 8/9/10合规基线检查
cis	hc_iis_djbh	等保三级-IIS合规基线检查
cis	hc_informix_djbh	等保三级-Informix合规基线检查
cis	hc_jboss_djbh	等保三级-Jboss合规基线检查
cis	hc_mongo_djbh	等保三级-MongoDB合规基线检查
cis	hc_mssql_djbh	等保三级-SQL Server合规基线检查
cis	hc_mysql_djbh	等保三级-MySql合规基线检查
cis	hc_nginx_djbh	等保三级-Nginx合规基线检查

类型名称	子类型名称	描述
cis	hc_oracle_djbh	等保三级-Oracle合规基线检查
cis	hc_pgsql_djbh	等保三级-PostgreSql合规基线检查
cis	hc_redhat 6_djbh_l3	等保三级-Redhat Linux 6合规基线检查
cis	hc_redhat_djbh_l3	等保三级-Redhat Linux 7合规基线检查
cis	hc_redis_djbh	等保三级-Redis合规基线检查
cis	hc_suse 10_djbh_l3	等保三级-SUSE 10合规基线检查
cis	hc_suse 12_djbh_l3	等保三级-SUSE 12合规基线检查
cis	hc_suse_djbh_l3	等保三级-SUSE 11合规基线检查
cis	hc_ubuntu 14_djbh_l3	等保三级-Ubuntu 14合规基线检查
cis	hc_ubuntu_djbh_l3	等保三级-Ubuntu 16/18/20合规基线检查
cis	hc_was_djbh	等保三级-Websphere Application Server合规基线检查
cis	hc_weblogic_djbh	等保三级-Weblogic合规基线检查
cis	hc_win 2008_djbh_l3	等保三级-Windows 2008 R2合规基线检查
cis	hc_win 2012_djbh_l3	等保三级-Windows 2012 R2合规基线检查
cis	hc_win 2016_djbh_l3	等保三级-Windows 2016/2019 合规基线检查
cis	hc_aliyun_linux_djbh_l2	等保二级-Alibaba Cloud Linux/Aliyun Linux 2合规基线检查
cis	hc_centos 6_djbh_l2	等保二级-CentOS Linux 6合规基线检查
cis	hc_centos 7_djbh_l2	等保二级-CentOS Linux 7合规基线检查
cis	hc_debian_djbh_l2	等保二级-Debian Linux 8合规基线检查
cis	hc_redhat 7_djbh_l2	等保二级-Redhat Linux 7合规基线检查
cis	hc_ubuntu_djbh_l2	等保二级-Ubuntu16/18合规基线检查
cis	hc_win 2008_djbh_l2	等保二级-Windows 2008 R2合规基线检查
cis	hc_win 2012_djbh_l2	等保二级-Windows 2012 R2合规基线检查
cis	hc_win 2016_djbh_l2	等保二级-Windows 2016/2019 合规基线检查
cis	hc_aliyun_linux_cis	CIS标准-Alibaba Cloud Linux/Aliyun Linux 2安全基线检查

类型名称	子类型名称	描述
cis	hc_centos 6_cis_rules	CIS标准-CentOS Linux 6安全基线检查
cis	hc_centos 7_cis_rules	CIS标准-CentOS Linux 7安全基线检查
cis	hc_centos 8_cis_rules	CIS标准-CentOS Linux 8安全基线检查
cis	hc_debian 8_cis_rules	CIS标准-Debian Linux 8安全基线检查
cis	hc_ubuntu 14_cis_rules	CIS标准-Ubuntu 14安全基线检查
cis	hc_ubuntu 16_cis_rules	CIS标准-Ubuntu 16/18/20安全基线检查
cis	hc_win 2008_cis_rules	CIS标准-Windows Server 2008 R2安全基线检查
cis	hc_win 2012_cis_rules	CIS标准-Windows Server 2012 R2安全基线检查
cis	hc_win 2016_cis_rules	CIS标准-Windows Server 2016/2019 R2安全基线检查
cis	hc_kylin_djbh_l3	等保三级-麒麟合规基线检查
cis	hc_uos_djbh_l3	等保三级-Uos合规基线检查
hc_best_security	hc_aliyun_linux	阿里云标准-Alibaba Cloud Linux/Aliyun Linux 2安全基线检查
hc_best_security	hc_centos 6	阿里云标准-CentOS Linux 6安全基线检查
hc_best_security	hc_centos 7	阿里云标准-CentOS Linux 7/8安全基线检查
hc_best_security	hc_debian	阿里云标准-Debian Linux 8/9/10安全基线检查
hc_best_security	hc_redhat 6	阿里云标准-Redhat Linux 6安全基线检查
hc_best_security	hc_redhat 7	阿里云标准-Redhat Linux 7/8安全基线检查
hc_best_security	hc_ubuntu	阿里云标准-Ubuntu安全基线检查
hc_best_security	hc_windows_2008	阿里云标准-Windows 2008 R2安全基线检查
hc_best_security	hc_windows_2012	阿里云标准-Windows 2012 R2安全基线检查
hc_best_security	hc_windows_2016	阿里云标准-Windows 2016/2019 安全基线检查

类型名称	子类型名称	描述
hc_best_security	hc_db_mssql	阿里云标准-SQL server安全基线检查
hc_best_security	hc_memcached_ali	阿里云标准-Memcached安全基线检查
hc_best_security	hc_mongodb	阿里云标准-MongoDB 3.x版本安全基线检查
hc_best_security	hc_mysql_ali	阿里云标准-Mysql安全基线检查
hc_best_security	hc_oracle	阿里云标准-Oracle 11g安全基线检查
hc_best_security	hc_pgsql_ali	阿里云标准-PostgreSql安全基线检查
hc_best_security	hc_redis_ali	阿里云标准-Redis安全基线检查
hc_best_security	hc_apache	阿里云标准-Apache安全基线检查
hc_best_security	hc_iis_8	阿里云标准-IIS 8安全基线检查
hc_best_security	hc_nginx_linux	阿里云标准-Nginx安全基线检查
hc_best_security	hc_suse 15	阿里云标准-SUSE Linux 15安全基线检查
hc_best_security	tomcat 7	阿里云标准-Apache Tomcat 安全基线检查
weak_password	hc_mongodb_pwd	弱口令-MongoDB登录弱口令检测（支持2.x版本）
weak_password	hc_weakpwd_ftp_linux	弱口令-FTP登录弱口令检查
weak_password	hc_weakpwd_linux_sys	弱口令-Linux系统登录弱口令检查
weak_password	hc_weakpwd_mongodb 3	弱口令-MongoDB登录弱口令检测
weak_password	hc_weakpwd_mssql	弱口令-SQL Server数据库登录弱口令检查

类型名称	子类型名称	描述
weak_password	hc_weakpwd_mysql_linux	弱口令-Mysql数据库登录弱口令检查
weak_password	hc_weakpwd_mysql_win	弱口令-Mysql数据库登录弱口令检查（Windows版）
weak_password	hc_weakpwd_openldap	弱口令-Openldap登录弱口令检查
weak_password	hc_weakpwd_oracle	弱口令-Oracle登录弱口令检测
weak_password	hc_weakpwd_pgsql	弱口令-PostgreSQL数据库登录弱口令检查
weak_password	hc_weakpwd_pptp	弱口令-pptpd服务登录弱口令检查
weak_password	hc_weakpwd_redis_linux	弱口令-Redis数据库登录弱口令检查
weak_password	hc_weakpwd_rsync	弱口令-rsync服务登录弱口令检查
weak_password	hc_weakpwd_svn	弱口令-svn服务登录弱口令检查
weak_password	hc_weakpwd_tomcat_linux	弱口令-Apache Tomcat控制台弱口令检查
weak_password	hc_weakpwd_vnc	弱口令-VncServer弱口令检查
weak_password	hc_weakpwd_weblogic	弱口令-Weblogic 12c登录弱口令检测
weak_password	hc_weakpwd_win_sys	弱口令-Windows系统登录弱口令检查

安全日志状态码

状态值	描述
1	未修复
2	修复失败
3	回滚失败
4	修复中
5	回滚中

状态值	描述
6	验证中
7	修复成功
8	修复成功待重启
9	回滚成功
10	忽略
11	回滚成功待重启
12	已不存在
20	已失效

安全告警状态码

状态值	描述
1	待处理
2	已忽略
4	已确认
8	已标记误报
16	处理中
32	处理完毕
64	已经过期
128	已经删除
512	自动拦截中
513	自动拦截完毕

基线日志状态码

状态值	描述
1	未通过
2	验证中
3	已通过
5	已经失效

状态值	描述
6	已经忽略
7	修复中

安全告警日志

字段名	说明	示例
data_source	数据源。更多信息，请参见安全告警data_source列表。	aegis_login_log
level	告警事件的危险等级。取值（以下等级排序按照严重等级递减）： • serious：紧急 • suspicious：可疑 • remind：提醒	suspicious
name	告警名称。	Suspicious Process-SSH-based Remote Execution of Non-interactive Commands
op	操作信息。取值： • new：新增 • dealing：处理	new
status	状态信息。更多信息，请参见安全日志状态码。	1
uuid	产生告警的服务器UUID。	12345-b7ca-4a0a-9267-123456
detail	告警详细信息。 说明 告警类型不同，日志中的detail字段包含的内容也不同。如果您在查看告警日志时，对detail字段中的参数有疑问，您可以提交工单咨询。	由于detail字段内容较长，以下示例截取了非常用登录地登录服务器的告警日志中，detail字段的部分内容：{"loginSourceIp":"120.27.XX.XX","loginTimes":1,"type":"login_common_location","loginDestinationPort":22,"loginUser":"aike","protocol":2,"protocolName":"SSH","location":"青岛市"}
unique_info	告警的唯一标识。	2536dd765f804916a1fa3b9516b5****

安全告警data_source列表

值	描述
aegis_suspicious_event	主机异常
aegis_suspicious_file_v2	WebShell

值	描述
aegis_login_log	异常登录
security_event	云安全中心异常事件

主机日志

进程启动日志

字段名	说明	示例
uuid	进程所在服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****
ip	客户端主机的IP地址。	1.2.XX.XX
cmdline	进程启动的完整命令行。	cmd.exe /C "netstat -ano “
username	用户名。	administrator
uid	用户ID。	123
pid	进程ID。	7100
filename	进程文件名。	cmd.exe
filepath	进程文件完整路径。	C:/Windows/SysWOW64/cmd.exe
groupname	用户组。	group1
ppid	父进程ID。	2296
pfilename	父进程文件名。	client.exe
pfilepath	父进程文件完整路径。	D:/client/client.exe
		[{ "9883":"bash -c kill -0 -- -'6274'" }, { "19617":"/opt/java8/bin/java -Dproc_nodemanager -Xmx8192m -Dhdp.version=2.6.XX.XX-292 -Dhadoop.log.dir=/var/log/hadoop-yarn/yarn -Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.home.dir= -Dyarn.id.str=yarn -Dhadoop.root.logger=INFO,EWMA,RFA -

字段名	说明	示例
cmd_chain	进程链。	-Dhadoop.root.logger=INFO,EWMA,RFA -Dyarn.root.logger=INFO,EWMA,RFA -Djava.library.path=:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -Dyarn.policy.file=hadoop-policy.xml -Djava.io.tmpdir=/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -server -Dnm.audit.logger=INFO,NMAUDIT -Dnm.audit.logger=INFO,NMAUDIT -Dhadoop.log.dir=/var/log/hadoop-yarn/yarn -Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.home.dir=/usr/hdp/2.6.XX.XX-292/hadoop-yarn -Dhadoop.home.dir=/usr/hdp/2.6.XX.XX-292/hadoop -Dhadoop.root.logger=INFO,EWMA,RFA -Dyarn.root.logger=INFO,EWMA,RFA -Djava.library.path=:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -classpath /usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/./:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/lib/*:/usr/hdp/2.6.XX.XX-

字段名	说明	示例
		292/hadoop-hdfs/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-mapreduce/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-mapreduce/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop/conf/nm-config/log4j.properties org.apache.hadoop.yarn.server.nodemanager.NodeManager" }]
containerhostname	容器内服务器名称。	gamify-answer-bol-5-6876d5dc78-vf****
containerpid	容器内进程ID。	0
containerimageid	镜像ID。	sha256:7fee4a991f7c41c5511234dfea37a2a5c70c894fa7b4ca5c08d9fad74077****
containerimagename	镜像名称。	registry-vpc.cn-north-2-gov-1.aliyuncs.com/lippi-dingtalk/gamify-answer-bol-start:2020111714****
containername	容器名称。	k8s_gamify-answer-bol_gamify-answer-bol-5-6876d5dc78-vf6rb_study-gamify-answer-bol_483a1ed1-28b7-11eb-bc35-00163e010b62_0****
containerid	容器ID。	b564567427272d46f9b1cc4ade06a85fdf55075c06fdb870818d5925fa86****
cmd_chain_index	进程链索引，可以通过相同索引查找进程链。	P253
cmd_index	命令行每个参数的索引，每两个为一组，标识一个参数的起止索引。	0,3,5,8
comm	进程关联的命令名。	N/A
gid	进程组的ID。	0
parent_cmd_line	父进程的命令行。	/bin/sh -c ip a |grep inet|grep -v inet6|grep -v 127.0.0.1|grep -v 'inet 192.168.'|grep -v 'inet 10.'|awk '{print $2}'|sed 's#/[0-9]*##g'
pid_start_time	父进程的启动时间。	2022-01-12 15:27:46

字段名	说明	示例
srv_cmd	祖进程的命令行。	/www/server/panel/pyenv/bin/python /www/server/panel/BT-Task
stime	进程的启动时间。	2022-01-12 15:27:46

进程快照日志

字段名	说明	示例
uuid	进程所在服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****
ip	客户端主机的IP地址。	1.2.XX.XX
cmdline	进程启动的完整命令行。	cmd.exe /C "netstat -ano"
pid	进程ID。	7100
name	进程文件名。	cmd.exe
path	进程文件所在的完整路径。	C:/Windows/SysWOW64/cmd.exe
md5	进程文件名MD5。 说明 超过1 MB的进程文件不进行MD5计算。	d0424c22dfa03f6e4d5289f7f5934dd4
pname	父进程文件名。	client.exe
start_time	进程启动时间。内置字段。	2018-01-18 20:00:12
user	用户名。	administrator
uid	用户ID。	123

登录日志

说明 1分钟内的重复登录会被合并为1条日志，字段 `warn_count` 表示次数。

字段名	说明	示例
uuid	被登录的服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****
ip	客户端主机的IP地址。	1.2.XX.XX
warn_ip	登录来源IP地址。	1.2.XX.XX
warn_port	登录端口。	22

字段名	说明	示例
warn_type	登录类型。取值： • SSHLOGIN：SSH登录 • RDPLOGIN：远程桌面登录 • IPCLOGIN：IPC连接登录	SSHLOGIN
warn_user	登录用户名。	admin
warn_count	登录次数。1分钟内重复登录会被合并为1条日志。例如 `warn_count` 值为3表示这次登录前1分钟内还登录了2次。	3

暴力破解日志

字段名	说明	示例
uuid	被暴力破解的服务器UUID。	5d83b26b-b7ca-4a0a-9267-12*****
ip	服务器IP地址。	1.2.XX.XX
warn_ip	登录来源IP地址。	1.2..XX.XX
warn_port	登录端口。	22
warn_type	登录类型。取值： • SSHLOGIN：SSH登录 • RDPLOGIN：远程桌面登录 • IPCLOGIN：IPC连接登录	SSHLOGIN
warn_user	登录用户名。	admin
warn_count	失败登录次数。	3

网络连接日志

说明 服务器上每隔10秒到1分钟会收集变化的网络连接，而一个网络连接的状态收集从建立到结束过程中的部分状态。

字段名	说明	示例
uuid	服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****
ip	服务器IP地址。	1.2.XX.XX
src_ip	源IP地址。	1.2.XX.XX

字段名	说明	示例
src_port	源端口。	41897
dst_ip	目标IP地址。	1.2.XX.XX
dst_port	目标端口。	22
proc_name	进程名。	java
proc_path	进程路径。	/hsdata/jdk1.7.0_79/bin/java
proto	协议。取值： • tcp • udp • raw（表示raw socket）	tcp
status	连接状态。更多信息请参见网络连接状态描述列表。	5
		[{ "9883":"bash -c kill -0 -- -6274'" }, { "19617":"/opt/java8/bin/java -Dproc_nodemanager -Xmx8192m -Dhdp.version=2.6.XX.XX-292 -Dhadoop.log.dir=/var/log/hadoop-yarn/yarn -Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.home.dir= -Dyarn.id.str=yarn -Dhadoop.root.logger=INFO,EWMA,RFA -Dyarn.root.logger=INFO,EWMA,RFA -Djava.library.path=:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -Dyarn.policy.file=hadoop-policy.xml -

字段名	说明	示例
cmd_chain	进程链。	-Djava.io.tmpdir=/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -server -Dnm.audit.logger=INFO,NMAUDIT -Dnm.audit.logger=INFO,NMAUDIT -Dhadoop.log.dir=/var/log/hadoop-yarn/yarn -Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.home.dir=/usr/hdp/2.6.XX.XX-292/hadoop-yarn -Dhadoop.home.dir=/usr/hdp/2.6.XX.XX-292/hadoop -Dhadoop.root.logger=INFO,EWMA,RFA -Dyarn.root.logger=INFO,EWMA,RFA -Djava.library.path=:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -classpath /usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/./:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-mapreduce/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-mapreduce/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop/conf/nm-config/log4j.properties org.apache.hadoop.yarn.server.nodemanager.NodeManager"

字段名	说明	示例
pid	进程ID。	123
ppid	父进程ID。	1
container_hostname	容器内服务器名称。	gamify-answer-bol-5-6876d5dc78-v****
container_pid	容器内进程ID。	0
container_image_id	镜像ID。	sha256:7fee4a991f7c41c5511234dfea37a2a5c70c894fa7b4ca5c08d9fad74077****
container_image_name	镜像名称。	registry-vpc.cn-north-2-gov-1.aliyuncs.com/lippi-dingtalk/gamify-answer-bol-start:2020111714****
container_name	容器名称。	k8s_gamify-answer-bol_gamify-answer-bol-5-6876d5dc78-vf6rb_study-gamify-answer-bol_483a1ed1-28b7-11eb-bc35-00163e010b62_0****
container_id	容器ID。	b564567427272d46f9b1cc4ade06a85fdf55075c06fdb870818d5925fa86****
cmd_chain_index	进程链索引，可以通过相同索引查找进程链。	P3285
parent_proc_file_name	父进程的文件名。	/usr/bin/bash
proc_start_time	进程的启动时间。	N/A
srv_comm	祖进程关联的命令名。	python
uid	进程用户的ID。	-1
username	进程的用户名。	N/A

网络连接状态描述列表

状态值	描述
1	closed
2	listen
3	syn send
4	syn recv

状态值	描述
5	establisted
6	close wait
7	closing
8	fin_wait1
9	fin_wait2
10	time_wait
11	delete_tcb

端口监听快照

字段名	说明	示例
uuid	服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****
ip	服务器的IP地址。	1.2.XX.XX
proto	通信使用的协议。取值： • tcp • udp • raw（表示raw socket）	tcp
src_ip	监听的IP地址。	1.2.XX.XX
src_port	监听端口。	41897
pid	进程ID。	7100
proc_name	进程名。	kubelet

账号快照

说明 账号快照展示了在您资产中检测到的账号信息。

字段名	说明	示例
uuid	服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****
ip	服务器IP地址。	1.2.XX.XX
user	用户名称。	nscd

字段名	说明	示例
perm	是否拥有登录服务器root权限。取值： • 0：没有root权限。 • 1：有root权限。	0
home_dir	home目录。	/Users/abc
groups	用户所在的分组。不属于任何组时为 `N/A` 。	["users", "root"]
last_chg	密码最后的修改日期。	2017-08-24
shell	Linux的Shell命令。	/sbin/nologin
domain	Windows域。不属于任何域为 `N/A` 。	administrator
tty	登录的终端。账号从未登录过终端时为 `N/A` 。	pts/3
warn_time	密码到期提醒日期。永不提醒时为 `never` 。	2017-08-24
account_expire	账号过期日期。永不过期时为 `never` 。	2017-08-24
passwd_expire	密码过期日期。永不过期时为 `never` 。	2017-08-24
login_ip	最后一次登录的远程IP地址。账号从未登录时为 `N/A` 。	1.2.XX.XX
last_logon	最后一次登录的日期和时间。账号从未登录时为 `N/A` 。	2017-08-21 09:21:21
status	用户账号状态，取值： • 0：账号已被禁止登录 • 1：账号可正常登录	0

1.1. 使用前必读

云安全中心全量日志集中存放在专属Logstore（日志库）中。您可以在日志服务控制台中，储存云安全中心日志服务的项目sas-log-阿里云账户ID-区域名中找到专属Logstore。

云安全中心开通日志分析后，系统会自动在日志服务控制台创建专属于云安全中心的Logstore（Logstore名称为*sas-log*）并存储云安全中心的日志数据，请您注意不要误删。

> **注意** 如果误删Logstore，后台会提示sas-log日志库不存在，并且您当前Logstore的所有日志数据会丢失。这种情况下，您需提交工单重置处理。重置后您需重新开通日志分析服务后才可继续使用日志分析。已丢失的日志数据无法恢复。

日志库限制说明

- 您无法通过API或SDK等方式在数据库中写入数据，或者修改日志库的属性（例如存储周期等）。
- 开通云安全中心日志服务需要先付费购买后再开通SLS日志服务。
- 内置的报表可能会在以后更新并升级。
- 仅企业版和旗舰版用户支持查看网络日志，防病毒版和高级版用户不支持。防病毒版和高级版用户在云安全中心控制台**日志分析**页面仅能查看安全日志和主机日志。

日志存储的地域

开通日志分析后，云安全中心会自动创建3个Project用于存储云安全中心产生的日志数据。

下表说明了云安全中心自动创建的Project存储数据来源的地域。

日志分析Project所属地域	存储数据的来源地域
华东1（杭州）	中国内地
新加坡	海外
马来西亚（吉隆坡）	暂无

1.2. 开通日志分析

云安全中心日志分析功能为您提供准确实时的日志查询和日志分析能力。本文介绍如何开通日志分析。

背景信息

使用日志分析之前，您需要先在云安全中心控制台开通日志服务功能。

仅支持防病毒版、高级版、企业版和旗舰版用户在购买日志分析容量后使用该功能。免费版用户需要升级到防病毒版、高级版、企业版或旗舰版并购买日志分析容量后才能使用该功能。购买和升级云安全中心服务的操作，请参见购买云安全中心和升级与降配。各版本支持的功能详情，请参见功能特性。

> **注意** 云安全中心默认开启安全日志、网络日志、主机日志三大类日志。仅企业版和旗舰版用户支持查看网络日志，防病毒版和高级版用户不支持。防病毒版和高级版用户在云安全中心控制台**日志分析**页面仅能查看安全日志和主机日志。

在云安全中心控制台开通日志分析功能后，日志服务会为您自动创建云安全中心的专属日志库（Logstore）。您可以在日志服务控制台查看专属日志库的信息。日志库限制条件的详细内容请参见日志库限制说明。

> **说明** 开通日志分析功能需要额外付费。1 TB日志存储容量收取500元/月。根据《网络安全法》日志至少存储180天的要求，推荐每台服务器配置40 GB的日志存储容量。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**调查响应 > 日志分析**。
3. 如果您之前未授权云安全中心访问您的云资源，单击**立即授权**。

该操作是授权云安全中心访问您的云资源。授权成功后，访问控制服务会自动创建RAM角色：AliyunServiceRoleForSas，云安全中心使用此角色访问您其他产品中的云资源，为您的其他云资源提供安全防护。更多信息，请参见服务关联角色。

4. 在**开通日志服务**配置向导中，单击**立即开通**，完成日志服务开通。

5. 在**开通与购买**配置向导中，单击**立即开通**。
6. 在云安全中心购买页面，选择版本并设置**日志分析**容量。

您需要选择高级版、企业版或旗舰版。根据《网络安全法》日志至少存储180天的要求，推荐每台服务器配置40 GB的日志存储容量。

7. 单击**立即购买**。
8. 选中**云安全中心服务协议**并单击**去支付**完成支付。
9. 返回云安全中心控制台**日志分析**页面，单击**已完成开通**。

开通完成后，您可以开始使用云安全中心的日志分析服务。

1.3. 日志类别及参数说明

云安全中心日志服务默认开启安全日志、网络日志、主机日志三大类日志，全面实时防护您的资产。

云安全中心默认开启以下三大类日志：

- **安全日志**
  - 漏洞日志
  - 基线日志

- 安全告警日志

- **网络日志**
  - DNS解析日志
  - 本地DNS日志
  - 网络会话日志
  - Web访问日志

> **说明** 仅企业版和旗舰版用户支持查看网络日志，防病毒版和高级版用户不支持。防病毒版和高级版用户在云安全中心控制台**日志分析**页面仅能查看安全日志和主机日志。

- **主机日志**
  - 进程启动日志
  - 网络连接日志
  - 登录流水日志
  - 暴力破解日志
  - 进程快照
  - 账号快照
  - 端口快照

安全日志

安全日志参数说明见下表：

日志类型	主题（ __topic__ ）	描述	采集周期
漏洞日志	sas-vul-log	漏洞相关的日志。	实时采集。
基线日志	sas-hc-log	基线风险相关的日志。	实时采集。
安全告警日志	sas-security-log	安全告警相关的日志。	实时采集。

网络日志

网络日志参数说明见下表：

日志类型	主题（ __topic__ ）	描述	采集周期
DNS解析日志	sas-log-dns	外网DNS流量的相关日志。	延迟2小时采集。
本地DNS日志	local-dns	内网DNS流量相关的日志。	延迟1小时采集。
网络会话日志	sas-log-session	特定协议的网络日志。	延迟1小时采集。
Web访问日志	sas-log-http	服务器与外网通信的HTTP流量日志。	延迟1小时采集。

主机日志

主机日志参数说明见下表：

日志类型	主题（ __topic__ ）	描述	采集周期
进程启动日志	aegis-log-process	服务器上进程启动相关的日志。	实时采集，进程启动立刻上报。
网络连接日志	aegis-log-network	服务器连接的五元组相关的日志。	• Windows系统：实时采集。 • Linux系统：每隔10秒采集，增量上报。
登录流水日志	aegis-log-login	SSH、RDP登录成功日志。	实时采集。
暴力破解日志	aegis-log-crack	登录失败相关的日志。	实时采集。
进程快照	aegis-snapshot-process	服务器上进程快照信息。	资产指纹自动收集功能开启后才有数据。每台服务器一天非固定时间收集一次。
账号快照	aegis-snapshot-host	服务器上账户快照信息。	资产指纹自动收集功能开启后才有数据。每台服务器一天非固定时间收集一次。
端口快照	aegis-snapshot-port	服务器上端口侦听快照信息。	资产指纹自动收集功能开启后才有数据。每台服务器一天非固定时间收集一次。

1.4. 日志字段说明

本文档提供了云安全中心日志的字段说明。

实时数据

字段名	说明	示例
dir	网络连接方向。取值： • in：入方向 • out：出方向	in
src_ip	网络连接发起者的IP。 • dir为out时表示本机 • dir为in时表示对端主机	10.240.XX.XX
src_port	网络连接发起者的端口。	24680

字段名	说明	示例
dst_ip	网络连接接收者的IP。 • dir为out时表示对端主机 • dir为in时表示本机	10.240.XX.XX
dst_port	网络连接接收者端口。	22
status	网络连接状态。 说明 实时日志中该参数的取值为随机赋予，取值无任何意义，您无需关注。	2
type	实时网络连接的类型。取值： • connect：主动发起TCP connect连接 • accept：收到TCP连接 • listen：端口监听	listen

快照数据（资产指纹）

字段名	说明	示例
proc_path	进程路径。	"/usr/sbin/sshd"
proc_cmdline	进程命令行。	"/usr/sbin/sshd -D"
pid	进程ID。	1158
ppid	父进程ID。	1
dir	网络连接方向。取值： • in：入方向 • out：出方向	in
src_ip	网络连接发起者的IP。 • dir为out时表示本机 • dir为in时表示对端主机	10.240.XX.XX
src_port	网络连接发起者的端口。	24680
dst_ip	网络连接接收者的IP。 • dir为out时表示对端主机 • dir为in时表示本机	10.240.XX.XX
dst_port	网络连接接收者端口。	22

字段名	说明	示例
status	网络连接状态。取值： • 1：TCP_STATE_CLOSED（连接关闭/未打开） • 2：TCP_STATE_LISTEN（监听中） • 3：TCP_STATE_SYN_SENT（发送SYN包） • 4：TCP_STATE_SYN_RCVD（SYN包已接收） • 5：TCP_STATE_ESTABLISHED（已建立连接） • 6：TCP_STATE_CLOSE_WAIT（等待关闭） • 7：TCP_STATE_CLOSING（双方都在关闭连接） • 8：TCP_STATE_FIN_WAIT1（主动关闭方发送FIN等待ACK） • 9：TCP_STATE_FIN_WAIT2（主动关闭方收到ACK） • 10：TCP_STATE_LAST_ACK（被动关闭方等待ACK） • 11：TCP_STATE_TIME_WAIT（主动关闭方收到FIN并发送ACK）	2

网络日志

DNS解析日志

字段名	说明	示例
additional	additional字段，竖线分隔。	无
additional_num	additional字段数量。	0
answer	DNS回答信息，竖线分隔。	example.com A IN 52 1.2.XX.XX
answer_num	DNS回答信息数量。	1
authority	authority字段。	NS IN 17597
authority_num	authority字段数量。	1
client_subnet	客户端子网。	172.168.XX.XX

字段名	说明	示例
dst_ip	目标IP。	1.2.XX.XX
dst_port	目标端口。	53
in_out	数据的传输方向，取值： • in：流入 • out：流出	out
qid	查询ID。	12345
qname	查询域名。	example.com
qtype	查询类型。	A
query_datetime	查询时间戳（毫秒）。	1537840756263
rcode	返回代码。	0
region	来源区域ID。取值： • 1：北京 • 2：青岛 • 3：杭州 • 4：上海 • 5：深圳 • 6：其他	1
response_datetime	返回时间。	2018-09-25 09:59:16
src_ip	源IP地址。	1.2.XX.XX
src_port	源端口。	22

本地DNS日志

字段名	说明	示例
answer_rda	DNS回答信息，竖线分隔。	example.com
answer_ttl	DNS回答的时间周期，竖线分隔。	100
answer_type	DNS回答的类型，竖线分隔。	1
anwser_name	DNS回答的名称，竖线分隔。	example.com
dest_ip	目标IP地址。	1.2.XX.XX
dest_port	目标端口。	53

字段名	说明	示例
group_id	分组ID。	3
hostname	主机名。	hostname
id	查询的ID。	64588
instance_id	实例ID。	i-2zeg4zldn8zypsfg****
internet_ip	公网IP地址。	1.2.XX.XX
ip_ttl	IP的周期。	64
query_name	查询的域名。	example.com
query_type	查询的类型。	A
src_ip	源IP地址。	1.2.XX.XX
src_port	源端口。	1234
time	查询时间戳（秒）。	1537840756
time_usecond	响应耗时（微秒）。	49069
tunnel_id	通道ID。	514763

网络会话日志

字段名	说明	示例
asset_type	产生日志的资产。取值： • ECS • SLB • RDS	ECS
dst_ip	目标IP地址。	1.2.XX.XX
dst_port	目标端口。	53
proto	协议类型。取值： • tcp • udp	tcp
session_time	会话开始时间。	2018-09-25 09:59:49
src_ip	源IP地址。	1.2.XX.XX
src_port	源端口。	54

Web访问日志

字段名	说明	示例
content_length	消息实体的传输长度。单位为：字节。	123
dst_ip	目的IP地址。	1.2.XX.XX
dst_port	目的端口。	54
host	访问的主机。	47.XX.XX.158:8080
jump_location	重定向地址。	123
method	HTTP请求方式。	GET
referer	客户端向服务器发送请求时的HTTP referer，告知服务器访问来源的HTTP连接。	www.example.com
request_datetime	请求时间。	2018-09-25 09:58:37
ret_code	返回状态值。	200
rqs_content_type	请求内容类型。	text/plain;charset=utf-8
rsp_content_type	响应内容类型。	text/plain; charset=utf-8
src_ip	源IP地址。	1.2.XX.XX
src_port	源端口。	54
uri	请求URI。	/report
user_agent	向用户客户端发起的请求。	okhttp/3.2.0
x_forward_for	路由跳转信息。	1.2.XX.XX

安全日志

漏洞日志

字段名	说明	示例
name	漏洞名称。	oval:com.redhat.rhsa:def:20182390
alias_name	漏洞别名。	RHSA-2018:2390: kernel security and bug fix update

字段名	说明	示例
op	漏洞的处理动作。取值： • new：新增 • verify：验证 • fix：修复	new
status	漏洞状态信息。	1
tag	漏洞的标签。取值： • oval：Linux软件漏洞 • system：Windows系统漏洞 • cms：Web-CMS漏洞 说明 其他类型的漏洞的标签为随机字符串。	oval
type	漏洞类型。取值： • sys：windows系统漏洞 • cve：Linux软件漏洞 • cms：Web-CMS漏洞 • emg：紧急漏洞	sys
uuid	服务器UUID。	1234-b7ca-4a0a-9267-12****

基线日志

字段名	说明	示例
level	风险项级别。取值： • high：高 • mediam：中 • low：低	low
op	操作信息。取值： • new：新增 • verity：验证	new
risk_name	风险项名称。	密码策略合规检测
status	状态信息。更多信息，请参见安全日志状态码。	1
sub_type_alias	子类型别名（中文）。	系统账户安全
sub_type_name	子类型名称。	system_account_security

字段名	说明	示例
type_name	检测类型名称。	account
type_alias	类型别名（中文）。	cis
uuid	检测出当前风险项的服务器UUID。	12345-b7ca-4a0a-9267-123456

基线类型及子类型列表

类型名称	子类型名称	描述
hc_exploit	hc_exploit_redis	高危风险利用-Redis未授权访问高危风险
hc_exploit	hc_exploit_activemq	高危风险利用-ActiveMQ未授权访问高危风险
hc_exploit	hc_exploit_couchdb	高危风险利用-CouchDB未授权访问高危风险
hc_exploit	hc_exploit_docker	高危风险利用-Docker未授权访问高危风险
hc_exploit	hc_exploit_es	高危风险利用-Elasticsearch未授权访问高危风险
hc_exploit	hc_exploit_hadoop	高危风险利用-Hadoop未授权访问高危风险
hc_exploit	hc_exploit_jboss	高危风险利用-Jboss未授权访问高危风险
hc_exploit	hc_exploit_jenkins	高危风险利用-Jenkins未授权访问高危风险
hc_exploit	hc_exploit_k8s_api	高危风险利用Kubernetes-Apiserver未授权访问高危风险
hc_exploit	hc_exploit_ldap	高危风险利用-LDAP未授权访问高危风险（Windows环境）
hc_exploit	hc_exploit_ldap_linux	高危风险利用-openLDAP未授权访问高危风险（Linux环境）
hc_exploit	hc_exploit_memcache	高危风险利用-Memcached未授权访问高危风险
hc_exploit	hc_exploit_mongo	高危风险利用-Mongodb未授权访问高危风险
hc_exploit	hc_exploit_pgsql	高危风险利用-Postgresql未授权访问高危风险基线
hc_exploit	hc_exploit_rabbitmq	高危风险利用-RabbitMQ未授权访问高危风险
hc_exploit	hc_exploit_rsync	高危风险利用-rsync未授权访问高危风险
hc_exploit	hc_exploit_tomcat	高危风险利用-Apache Tomcat AJP文件包含漏洞风险
hc_exploit	hc_exploit_zookeeper	高危风险利用-ZooKeeper未授权访问高危风险
hc_container	hc_docker	阿里云标准-Docker安全基线检查

类型名称	子类型名称	描述
hc_container	hc_middleware_ack_master	CIS标准-Kubernetes(ACK) Master节点安全基线检查
hc_container	hc_middleware_ack_node	CIS标准-Kubernetes(ACK) Node节点安全基线检查
hc_container	hc_middleware_k8s	阿里云标准-Kubernetes-Master安全基线检查
hc_container	hc_middleware_k8s_node	阿里云标准-Kubernetes-Node安全基线检查
cis	hc_suse 15_djbh	等保三级-SUSE 15合规基线检查
cis	hc_aliyun_linux3_djbh_l3	等保三级-Alibaba Cloud Linux 3合规基线检查
cis	hc_aliyun_linux_djbh_l3	等保三级-Alibaba Cloud Linux/Aliyun Linux 2合规基线检查
cis	hc_bind_djbh	等保三级-Bind合规基线检查
cis	hc_centos 6_djbh_l3	等保三级-CentOS Linux 6合规基线检查
cis	hc_centos 7_djbh_l3	等保三级-CentOS Linux 7合规基线检查
cis	hc_centos 8_djbh_l3	等保三级-CentOS Linux 8合规基线检查
cis	hc_debian_djbh_l3	等保三级-Debian Linux 8/9/10合规基线检查
cis	hc_iis_djbh	等保三级-IIS合规基线检查
cis	hc_informix_djbh	等保三级-Informix合规基线检查
cis	hc_jboss_djbh	等保三级-Jboss合规基线检查
cis	hc_mongo_djbh	等保三级-MongoDB合规基线检查
cis	hc_mssql_djbh	等保三级-SQL Server合规基线检查
cis	hc_mysql_djbh	等保三级-MySql合规基线检查
cis	hc_nginx_djbh	等保三级-Nginx合规基线检查
cis	hc_oracle_djbh	等保三级-Oracle合规基线检查
cis	hc_pgsql_djbh	等保三级-PostgreSql合规基线检查
cis	hc_redhat 6_djbh_l3	等保三级-Redhat Linux 6合规基线检查
cis	hc_redhat_djbh_l3	等保三级-Redhat Linux 7合规基线检查
cis	hc_redis_djbh	等保三级-Redis合规基线检查
cis	hc_suse 10_djbh_l3	等保三级-SUSE 10合规基线检查
cis	hc_suse 12_djbh_l3	等保三级-SUSE 12合规基线检查

类型名称	子类型名称	描述
cis	hc_suse_djbh_l3	等保三级-SUSE 11合规基线检查
cis	hc_ubuntu 14_djbh_l3	等保三级-Ubuntu 14合规基线检查
cis	hc_ubuntu_djbh_l3	等保三级-Ubuntu 16/18/20合规基线检查
cis	hc_was_djbh	等保三级-Websphere Application Server合规基线检查
cis	hc_weblogic_djbh	等保三级-Weblogic合规基线检查
cis	hc_win 2008_djbh_l3	等保三级-Windows 2008 R2合规基线检查
cis	hc_win 2012_djbh_l3	等保三级-Windows 2012 R2合规基线检查
cis	hc_win 2016_djbh_l3	等保三级-Windows 2016/2019 合规基线检查
cis	hc_aliyun_linux_djbh_l2	等保二级-Alibaba Cloud Linux/Aliyun Linux 2合规基线检查
cis	hc_centos 6_djbh_l2	等保二级-CentOS Linux 6合规基线检查
cis	hc_centos 7_djbh_l2	等保二级-CentOS Linux 7合规基线检查
cis	hc_debian_djbh_l2	等保二级-Debian Linux 8合规基线检查
cis	hc_redhat 7_djbh_l2	等保二级-Redhat Linux 7合规基线检查
cis	hc_ubuntu_djbh_l2	等保二级-Ubuntu16/18合规基线检查
cis	hc_win 2008_djbh_l2	等保二级-Windows 2008 R2合规基线检查
cis	hc_win 2012_djbh_l2	等保二级-Windows 2012 R2合规基线检查
cis	hc_win 2016_djbh_l2	等保二级-Windows 2016/2019 合规基线检查
cis	hc_aliyun_linux_cis	CIS标准-Alibaba Cloud Linux/Aliyun Linux 2安全基线检查
cis	hc_centos 6_cis_rules	CIS标准-CentOS Linux 6安全基线检查
cis	hc_centos 7_cis_rules	CIS标准-CentOS Linux 7安全基线检查
cis	hc_centos 8_cis_rules	CIS标准-CentOS Linux 8安全基线检查
cis	hc_debian 8_cis_rules	CIS标准-Debian Linux 8安全基线检查
cis	hc_ubuntu 14_cis_rules	CIS标准-Ubuntu 14安全基线检查
cis	hc_ubuntu 16_cis_rules	CIS标准-Ubuntu 16/18/20安全基线检查
cis	hc_win 2008_cis_rules	CIS标准-Windows Server 2008 R2安全基线检查

类型名称	子类型名称	描述
cis	hc_win 2012_cis_rules	CIS标准-Windows Server 2012 R2安全基线检查
cis	hc_win 2016_cis_rules	CIS标准-Windows Server 2016/2019 R2安全基线检查
cis	hc_kylin_djbh_l3	等保三级-麒麟合规基线检查
cis	hc_uos_djbh_l3	等保三级-Uos合规基线检查
hc_best_security	hc_aliyun_linux	阿里云标准-Alibaba Cloud Linux/Aliyun Linux 2安全基线检查
hc_best_security	hc_centos 6	阿里云标准-CentOS Linux 6安全基线检查
hc_best_security	hc_centos 7	阿里云标准-CentOS Linux 7/8安全基线检查
hc_best_security	hc_debian	阿里云标准-Debian Linux 8/9/10安全基线检查
hc_best_security	hc_redhat 6	阿里云标准-Redhat Linux 6安全基线检查
hc_best_security	hc_redhat 7	阿里云标准-Redhat Linux 7/8安全基线检查
hc_best_security	hc_ubuntu	阿里云标准-Ubuntu安全基线检查
hc_best_security	hc_windows_2008	阿里云标准-Windows 2008 R2安全基线检查
hc_best_security	hc_windows_2012	阿里云标准-Windows 2012 R2安全基线检查
hc_best_security	hc_windows_2016	阿里云标准-Windows 2016/2019 安全基线检查
hc_best_security	hc_db_mssql	阿里云标准-SQL server安全基线检查
hc_best_security	hc_memcached_ali	阿里云标准-Memcached安全基线检查
hc_best_security	hc_mongodb	阿里云标准-MongoDB 3.x版本安全基线检查
hc_best_security	hc_mysql_ali	阿里云标准-Mysql安全基线检查
hc_best_security	hc_oracle	阿里云标准-Oracle 11g安全基线检查

类型名称	子类型名称	描述
hc_best_security	hc_pgsql_ali	阿里云标准-PostgreSql安全基线检查
hc_best_security	hc_redis_ali	阿里云标准-Redis安全基线检查
hc_best_security	hc_apache	阿里云标准-Apache安全基线检查
hc_best_security	hc_iis_8	阿里云标准-IIS 8安全基线检查
hc_best_security	hc_nginx_linux	阿里云标准-Nginx安全基线检查
hc_best_security	hc_suse 15	阿里云标准-SUSE Linux 15安全基线检查
hc_best_security	tomcat 7	阿里云标准-Apache Tomcat 安全基线检查
weak_password	hc_mongodb_pwd	弱口令-MongoDB登录弱口令检测（支持2.x版本）
weak_password	hc_weakpwd_ftp_linux	弱口令-FTP登录弱口令检查
weak_password	hc_weakpwd_linux_sys	弱口令-Linux系统登录弱口令检查
weak_password	hc_weakpwd_mongodb 3	弱口令-MongoDB登录弱口令检测
weak_password	hc_weakpwd_mssql	弱口令-SQL Server数据库登录弱口令检查
weak_password	hc_weakpwd_mysql_linux	弱口令-Mysql数据库登录弱口令检查
weak_password	hc_weakpwd_mysql_win	弱口令-Mysql数据库登录弱口令检查（Windows版）
weak_password	hc_weakpwd_openldap	弱口令-Openldap登录弱口令检查
weak_password	hc_weakpwd_oracle	弱口令-Oracle登录弱口令检测
weak_password	hc_weakpwd_pgsql	弱口令-PostgreSQL数据库登录弱口令检查

类型名称	子类型名称	描述
weak_password	hc_weakpwd_pptp	弱口令-pptpd服务登录弱口令检查
weak_password	hc_weakpwd_redis_linux	弱口令-Redis数据库登录弱口令检查
weak_password	hc_weakpwd_rsync	弱口令-rsync服务登录弱口令检查
weak_password	hc_weakpwd_svn	弱口令-svn服务登录弱口令检查
weak_password	hc_weakpwd_tomcat_linux	弱口令-Apache Tomcat控制台弱口令检查
weak_password	hc_weakpwd_vnc	弱口令-VncServer弱口令检查
weak_password	hc_weakpwd_weblogic	弱口令-Weblogic 12c登录弱口令检测
weak_password	hc_weakpwd_win_sys	弱口令-Windows系统登录弱口令检查

安全日志状态码

状态值	描述
1	未修复
2	修复失败
3	回滚失败
4	修复中
5	回滚中
6	验证中
7	修复成功
8	修复成功待重启
9	回滚成功
10	忽略
11	回滚成功待重启
12	已不存在

状态值	描述
20	已失效

安全告警状态码

状态值	描述
1	待处理
2	已忽略
4	已确认
8	已标记误报
16	处理中
32	处理完毕
64	已经过期
128	已经删除
512	自动拦截中
513	自动拦截完毕

基线日志状态码

状态值	描述
1	未通过
2	验证中
3	已通过
5	已经失效
6	已经忽略
7	修复中

安全告警日志

字段名	说明	示例
data_source	数据源。更多信息，请参见安全告警data_source列表。	aegis_login_log

字段名	说明	示例
level	告警事件的危险等级。取值（以下等级排序按照严重等级递减）： • serious：紧急 • suspicious：可疑 • remind：提醒	suspicious
name	告警名称。	Suspicious Process-SSH-based Remote Execution of Non-interactive Commands
op	操作信息。取值： • new：新增 • dealing：处理	new
status	状态信息。更多信息，请参见安全日志状态码。	1
uuid	产生告警的服务器UUID。	12345-b7ca-4a0a-9267-123456
detail	告警详细信息。 说明 告警类型不同，日志中的detail字段包含的内容也不同。如果您在查看告警日志时，对detail字段中的参数有疑问，您可以提交工单咨询。	由于detail字段内容较长，以下示例截取了非常用登录地登录服务器的告警日志中，detail字段的部分内容：{"loginSourceIp":"120.27.XX.XX","loginTimes":1,"type":"login_common_location","loginDestinationPort":22,"loginUser":"aike","protocol":2,"protocolName":"SSH","location":"青岛市"}
unique_info	告警的唯一标识。	2536dd765f804916a1fa3b9516b5****

安全告警data_source列表

值	描述
aegis_suspicious_event	主机异常
aegis_suspicious_file_v2	WebShell
aegis_login_log	异常登录
security_event	云安全中心异常事件

主机日志

进程启动日志

字段名	说明	示例
uuid	进程所在服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****

字段名	说明	示例
ip	客户端主机的IP地址。	1.2.XX.XX
cmdline	进程启动的完整命令行。	cmd.exe /C "netstat -ano “
username	用户名。	administrator
uid	用户ID。	123
pid	进程ID。	7100
filename	进程文件名。	cmd.exe
filepath	进程文件完整路径。	C:/Windows/SysWOW64/cmd.exe
groupname	用户组。	group1
ppid	父进程ID。	2296
pfilename	父进程文件名。	client.exe
pfilepath	父进程文件完整路径。	D:/client/client.exe
		[{ "9883":"bash -c kill -0 -- -'6274'" }, { "19617":"/opt/java8/bin/java -Dproc_nodemanager -Xmx8192m -Dhdp.version=2.6.XX.XX-292 -Dhadoop.log.dir=/var/log/hadoop-yarn/yarn -Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.home.dir= -Dyarn.id.str=yarn -Dhadoop.root.logger=INFO,EWMA,RFA -Dyarn.root.logger=INFO,EWMA,RFA -Djava.library.path=:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-

字段名	说明	示例
cmd_chain	进程链。	-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -Dyarn.policy.file=hadoop-policy.xml -Djava.io.tmpdir=/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -server -Dnm.audit.logger=INFO,NMAUDIT -Dnm.audit.logger=INFO,NMAUDIT -Dhadoop.log.dir=/var/log/hadoop-yarn/yarn -Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.home.dir=/usr/hdp/2.6.XX.XX-292/hadoop-yarn -Dhadoop.home.dir=/usr/hdp/2.6.XX.XX-292/hadoop -Dhadoop.root.logger=INFO,EWMA,RFA -Dyarn.root.logger=INFO,EWMA,RFA -Djava.library.path=:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -classpath /usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/./:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-mapreduce/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-mapreduce/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop/conf/nm-

字段名	说明	示例
		config/log4j.properties org.apache.hadoop.yarn.server.nodemanager.NodeManager" }]
containerhostname	容器内服务器名称。	gamify-answer-bol-5-6876d5dc78-vf****
containerpid	容器内进程ID。	0
containerimageid	镜像ID。	sha256:7fee4a991f7c41c5511234dfea37a2a5c70c894fa7b4ca5c08d9fad74077****
containerimagename	镜像名称。	registry-vpc.cn-north-2-gov-1.aliyuncs.com/lippi-dingtalk/gamify-answer-bol-start:2020111714****
containername	容器名称。	k8s_gamify-answer-bol_gamify-answer-bol-5-6876d5dc78-vf6rb_study-gamify-answer-bol_483a1ed1-28b7-11eb-bc35-00163e010b62_0****
containerid	容器ID。	b564567427272d46f9b1cc4ade06a85fdf55075c06fdb870818d5925fa86****
cmd_chain_index	进程链索引，可以通过相同索引查找进程链。	P253
cmd_index	命令行每个参数的索引，每两个为一组，标识一个参数的起止索引。	0,3,5,8
comm	进程关联的命令名。	N/A
gid	进程组的ID。	0
parent_cmd_line	父进程的命令行。	/bin/sh -c ip a |grep inet|grep -v inet6|grep -v 127.0.0.1|grep -v 'inet 192.168.'|grep -v 'inet 10.'|awk '{print $2}'|sed 's#/[0-9]*##g'
pid_start_time	父进程的启动时间。	2022-01-12 15:27:46
srv_cmd	祖进程的命令行。	/www/server/panel/pyenv/bin/python /www/server/panel/BT-Task
stime	进程的启动时间。	2022-01-12 15:27:46

进程快照日志

字段名	说明	示例
uuid	进程所在服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****

字段名	说明	示例
ip	客户端主机的IP地址。	1.2.XX.XX
cmdline	进程启动的完整命令行。	cmd.exe /C "netstat -ano"
pid	进程ID。	7100
name	进程文件名。	cmd.exe
path	进程文件所在的完整路径。	C:/Windows/SysWOW64/cmd.exe
md5	进程文件名MD5。 **说明** 超过1 MB的进程文件不进行MD5计算。	d0424c22dfa03f6e4d5289f7f5934dd4
pname	父进程文件名。	client.exe
start_time	进程启动时间。内置字段。	2018-01-18 20:00:12
user	用户名。	administrator
uid	用户ID。	123

登录日志

说明 1分钟内的重复登录会被合并为1条日志，字段 `warn_count` 表示次数。

字段名	说明	示例
uuid	被登录的服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****
ip	客户端主机的IP地址。	1.2.XX.XX
warn_ip	登录来源IP地址。	1.2.XX.XX
warn_port	登录端口。	22
warn_type	登录类型。取值： • SSHLOGIN：SSH登录 • RDPLOGIN：远程桌面登录 • IPCLOGIN：IPC连接登录	SSHLOGIN
warn_user	登录用户名。	admin

字段名	说明	示例
warn_count	登录次数。1分钟内重复登录会被合并为1条日志。例如 `warn_count` 值为3表示这次登录前1分钟内还登录了2次。	3

暴力破解日志

字段名	说明	示例
uuid	被暴力破解的服务器UUID。	5d83b26b-b7ca-4a0a-9267-12*****
ip	服务器IP地址。	1.2.XX.XX
warn_ip	登录来源IP地址。	1.2..XX.XX
warn_port	登录端口。	22
warn_type	登录类型。取值： • SSHLOGIN：SSH登录 • RDPLOGIN：远程桌面登录 • IPCLOGIN：IPC连接登录	SSHLOGIN
warn_user	登录用户名。	admin
warn_count	失败登录次数。	3

网络连接日志

说明 服务器上每隔10秒到1分钟会收集变化的网络连接，而一个网络连接的状态收集从建立到结束过程中的部分状态。

字段名	说明	示例
uuid	服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****
ip	服务器IP地址。	1.2.XX.XX
src_ip	源IP地址。	1.2.XX.XX
src_port	源端口。	41897
dst_ip	目标IP地址。	1.2.XX.XX
dst_port	目标端口。	22
proc_name	进程名。	java
proc_path	进程路径。	/hsdata/jdk1.7.0_79/bin/java

字段名	说明	示例
proto	协议。取值： • tcp • udp • raw（表示raw socket）	tcp
status	连接状态。更多信息请参见网络连接状态描述列表。	5
		[{ "9883":"bash -c kill -0 -- - '6274'" }, { "19617":"/opt/java8/bin/java - Dproc_nodemanager -Xmx8192m - Dhdp.version=2.6.XX.XX-292 - Dhadoop.log.dir=/var/log/hadoop- yarn/yarn - Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager- s-tencentyun-10-54-42-64.hx.log - Dyarn.log.file=yarn-yarn-nodemanager-s- tencentyun-10-54-42-64.hx.log - Dyarn.home.dir= -Dyarn.id.str=yarn - Dhadoop.root.logger=INFO,EWMA,RFA - Dyarn.root.logger=INFO,EWMA,RFA - Djava.library.path=:/usr/hdp/2.6.XX.XX- 292/hadoop/lib/native/Linux-amd64- 64:/usr/hdp/2.6.XX.XX- 292/hadoop/lib/native/Linux-amd64- 64:/usr/hdp/2.6.XX.XX- 292/hadoop/lib/native:/var/lib/ambari- agent/tmp/hadoop_java_io_tmpdir:/usr/hdp /2.6.XX.XX-292/hadoop/lib/native/Linux- amd64-64:/usr/hdp/2.6.XX.XX- 292/hadoop/lib/native/Linux-amd64- 64:/usr/hdp/2.6.XX.XX- 292/hadoop/lib/native:/var/lib/ambari- agent/tmp/hadoop_java_io_tmpdir - Dyarn.policy.file=hadoop-policy.xml - Djava.io.tmpdir=/var/lib/ambari- agent/tmp/hadoop_java_io_tmpdir -server -Dnm.audit.logger=INFO,NMAUDIT - Dnm.audit.logger=INFO,NMAUDIT - Dhadoop.log.dir=/var/log/hadoop- yarn/yarn - Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager- s-tencentyun-10-54-42-64.hx.log - Dyarn.log.file=yarn-yarn-nodemanager-s-

字段名	说明	示例
cmd_chain	进程链。	-Dyarn.log.file=yarn-yarn-nodemanager-s-ncentyun-10-54-42-64.hx.log -Dyarn.home.dir=/usr/hdp/2.6.XX.XX-292/hadoop-yarn -Dhadoop.home.dir=/usr/hdp/2.6.XX.XX-292/hadoop -Dhadoop.root.logger=INFO,EWMA,RFA -Dyarn.root.logger=INFO,EWMA,RFA -Djava.library.path=:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -classpath /usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/./:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-mapreduce/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-mapreduce/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop/conf/nm-config/log4j.properties org.apache.hadoop.yarn.server.nodemanager.NodeManager" }]
pid	进程ID。	123
ppid	父进程ID。	1

字段名	说明	示例
container_hostname	容器内服务器名称。	gamify-answer-bol-5-6876d5dc78-v****
container_pid	容器内进程ID。	0
container_image_id	镜像ID。	sha256:7fee4a991f7c41c5511234dfea37a2a5c70c894fa7b4ca5c08d9fad74077****
container_image_name	镜像名称。	registry-vpc.cn-north-2-gov-1.aliyuncs.com/lippi-dingtalk/gamify-answer-bol-start:2020111714****
container_name	容器名称。	k8s_gamify-answer-bol_gamify-answer-bol-5-6876d5dc78-vf6rb_study-gamify-answer-bol_483a1ed1-28b7-11eb-bc35-00163e010b62_0****
container_id	容器ID。	b564567427272d46f9b1cc4ade06a85fdf55075c06fdb870818d5925fa86****
cmd_chain_index	进程链索引，可以通过相同索引查找进程链。	P3285
parent_proc_file_name	父进程的文件名。	/usr/bin/bash
proc_start_time	进程的启动时间。	N/A
srv_comm	祖进程关联的命令名。	python
uid	进程用户的ID。	-1
username	进程的用户名。	N/A

网络连接状态描述列表

状态值	描述
1	closed
2	listen
3	syn send
4	syn recv
5	establisted
6	close wait
7	closing

状态值	描述
8	fin_wait1
9	fin_wait2
10	time_wait
11	delete_tcb

端口监听快照

字段名	说明	示例
uuid	服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****
ip	服务器的IP地址。	1.2.XX.XX
proto	通信使用的协议。取值： • tcp • udp • raw（表示raw socket）	tcp
src_ip	监听的IP地址。	1.2.XX.XX
src_port	监听端口。	41897
pid	进程ID。	7100
proc_name	进程名。	kubelet

账号快照

说明 账号快照展示了在您资产中检测到的账号信息。

字段名	说明	示例
uuid	服务器的UUID。	5d83b26b-b7ca-4a0a-9267-12****
ip	服务器IP地址。	1.2.XX.XX
user	用户名称。	nscd
perm	是否拥有登录服务器root权限。取值： • 0：没有root权限。 • 1：有root权限。	0
home_dir	home目录。	/Users/abc

字段名	说明	示例
groups	用户所在的分组。不属于任何组时为 `N/A` 。	["users", "root"]
last_chg	密码最后的修改日期。	2017-08-24
shell	Linux的Shell命令。	/sbin/nologin
domain	Windows域。不属于任何域为 `N/A` 。	administrator
tty	登录的终端。账号从未登录过终端时为 `N/A` 。	pts/3
warn_time	密码到期提醒日期。永不提醒时为 `never` 。	2017-08-24
account_expire	账号过期日期。永不过期时为 `never` 。	2017-08-24
passwd_expire	密码过期日期。永不过期时为 `never` 。	2017-08-24
login_ip	最后一次登录的远程IP地址。账号从未登录时为 `N/A` 。	1.2.XX.XX
last_logon	最后一次登录的日期和时间。账号从未登录时为 `N/A` 。	2017-08-21 09:21:21
status	用户账号状态，取值： • 0：账号已被禁止登录 • 1：账号可正常登录	0

1.5. 查询实时日志分析

1.5.1. 自定义日志查询与分析

在云安全中心日志分析页面，您可以对日志进行自定义查询与分析，查询多种复杂场景下的日志。本文介绍使用查询和分析语句的方法。

概述

在**调查响应 > 日志分析**页面的**查询/分析**框中，您可以对日志进行自定义查询和分析。日志查询语句由查询语法（Search）和分析语法（Analytics）两部分组成，中间通过|进行分隔。

在对日志进行自定义查询和分析时，查询语法和分析语法都是可选项。以下是查询语法和分析语法的说明：

- 查询（Search）：查询条件可以由关键词、模糊语句、数值、区间范围和组合条件等产生。如果为空或为星号（*），代表对该时间段所有数据不过滤任何条件、直接对所有查询结果进行统计。
- 分析（Analytics）：对查询结果或全量数据进行计算和统计。如果为空，代表只返回查询结果，不做统

计。

查询语法

日志服务查询语法支持全文查询和字段查询，查询框支持换行显示、语法高亮等功能。

- **全文查询**

  不需要指定字段，直接输入关键字查询。可以用双引号（""）包裹关键字，多个关键字之间以空格或 `and` 分割。以下是全文查询的常用示例：

  - **多关键字查询示例**

    搜索所有包含 `www.aliyundoc.com` 和 `404` 的日志。例如：

    ```
    www.aliyundoc.com 404
    ```

    或者：

    ```
    www.aliyundoc.com and 404
    ```

  - **条件查询示例**

    搜索所有包含 `www.aliyundoc.com` 并且包含 `error` 或者 `404` 的日志。例如：

    ```
    www.aliyundoc.com and (error or 404)
    ```

  - **后缀查询示例**

    搜索所有包含 `www.aliyundoc.com` 并且包含 `failed_` 开头关键字的日志。例如：

    ```
    www.aliyundoc.com and failed_*
    ```

    > **说明** 全文查询只支持后缀加 `*`，不支持前缀加 `*`。

- **字段查询**

  可实现数值类型字段的比较，格式为 `字段：值` 或 `字段>=值`，通过 `and`、`or` 等进行组合。也可以和全文搜索组合使用，同样通过 `and`、`or` 组合。

  日志服务支持基于字段进行更精准的查询。

  - **查询多字段示例**

    搜索所有**严重**等级的安全报警的日志。例如：

    ```
    __topic__ : sas-security-log and level: serious
    ```

    搜索某个客户端1.2.XX.XX上所有的SSH登录日志。例如：

    ```
    __topic__:aegis-log-login and ip:1.2.XX.XX and warn_type:SSHLOGIN
    ```

    > **说明** 每条日志中都包含一个 `__topic__` 字段表示主题，日志都是通过该字段来区分。示例中用的字段 `level`、`warn_type`、`ip` 等都是特定日志类型的字段。

- **查询数值字段示例**

  搜索所有响应时间超过1秒的本地DNS查询日志。例如：

  ```
  __topic__:local-dns and time_usecond > 1000000
  ```

  也支持区间查询，查询响应时间大于1秒且小于等于10秒的本地DNS查询日志。例如：

  ```
  __topic__:local-dns and time_usecond in [1000000,10000000]
  ```

详细的查询语法说明，请参见查询概述。

分析语法

您可以使用SQL 92语法对日志数据进行分析与统计。日志服务支持的语法与函数详细信息，请参见分析简介。

分析语句中可以省略SQL标准语法中的 `from` 表格名语句，即 `from log` 。

日志数据默认返回前100条，您可以使用LIMIT语法修改返回数据的条数。更多信息，请参见LIMIT子句。

基于日志时间的查询分析

每条日志都有一个内置字段 `__time__` ，表示这条日志的时间，以便在统计时进行基于时间的计算。其格式为Unix时间戳，本质是一个自从1970-01-01 00:00:00 UTC时间开始的累计过去的秒数。因此实际使用时，经过可选的计算后，需要格式化才可以展示。

- **选择并展示时间**

  这里在特定时间范围内，选择IP为 `1.2.XX.XX` 的最新10条登录日志，展示其中时间、来源IP以及登录类型。例如：

  ```
  __topic__: aegis-log-login and ip: 1.2.XX.XX
  | select date_format(__time__, '%Y-%m-%d %H:%i:%s') as time, warn_ip, warn_type
  order by __time__ desc
  limit 10
  ```

- **计算时间**

  查询登录过后的天数，可以使用 `__time__` 进行计算。例如：

  ```
  __topic__: aegis-log-login and ip: 1.2.XX.XX
  | select date_format(__time__, '%Y-%m-%d %H:%i:%s') as time, warn_ip, warn_type ,
  round((to_unixtime(now()) - __time__)/86400,1) as "days_passed"
  order by __time__ desc
  limit 10
  ```

  这里使用 `round((to_unixtime(now()) - __time__)/86400, 1)` ，先用 `to_unixtime` 将 `now()` 获取的时间转化为Unix时间戳，再与内置时间字段 `__time__` 相减，获得已经过去的时间秒数。最后除以86400，即一天的总秒数，再用函数 `round(data, 1)` 圆整为小数点后1位数的值，可得出每条攻击日志距离现在已经过去了几天。

- **基于特定时间分组统计**

  如果想知道特定时间范围内某个设备的登录趋势，可使用如下SQL：

```
__topic__: aegis-log-login and ip: 1.2.XX.XX
| select date_trunc('day', __time__) as dt,
count(1) as PV
group by dt
order by dt
```

这里使用内置字段 `__time__` ，传给函数 `date_trunc('day', ..)` 对时间按天对齐，将每条日志分组到了其所属的天的分区中进行统计总数 （`count(1)`） ，并按照分区时间块排序。函数 `date_trunc` 第一个参数提供更多其他单位进行对齐，包括 `second` 、 `miniute` 、 `hour` 、 `week` 、 `month` 、 `year` 等，函数说明，请参见日期和时间函数。

- **基于灵活时间分组统计**

  如果想知道更灵活的分组时间规律，例如整个账户下设备每5分钟的登录趋势，可以使用如下SQL:

```
__topic__: aegis-log-login
| select from_unixtime(__time__ - __time__% 300) as dt,
count(1) as PV
group by dt
order by dt
limit 1000
```

使用计算的内置时间字段计算 `__time__ - __time__% 300` ，同时使用函数 `from_unixtime` 进行格式化，将每条日志分组到了一个5分钟（300秒）的分区中进行统计总数 （`count(1)`） ，并按照分区时间块排序，获得前1000条，相当于选择时间内的前83小时的数据。

更多关于时间解析的函数，例如将一个时间格式转化为另外一个格式，需要使用 `date_parse` 与 `date_format` ，函数说明，请参见日期和时间函数。

基于客户端IP的查询分析

日志中 `warn_ip` 表示登录日志的登录源IP。

- 登录源国家分布

  查询某个设备登录来源的国家分布，例如：

```
__topic__: aegis-log-login and uuid: 12344567
| SELECT ip_to_country(warn_ip) as country,
count(1) as "登录次数"
group by country
```

这里先用函数 `ip_to_country` 得到这个登录源IP `warn_ip` 对应的国家信息。

- 登录者身份分布

  使用函数 `ip_to_province` 获得更详细的基于省份的登录者分布，例如：

```
__topic__: aegis-log-login and uuid: 12344567
| SELECT ip_to_province(warn_ip) as province,
        count(1) as "登录次数"
        group by province
```

这里使用了另外一个IP函数 `ip_to_province` 来获得一个IP的所属省份。如果是中国以外的IP地址，会尝试转化为其国家所属省份（州），但在选择中国地图展示时，会无法展示出来。

- 登录者热力分布

使用函数 `ip_to_geo` 获得一张登录者的热力图：

```
__topic__: aegis-log-login and uuid: 12344567
| SELECT ip_to_geo(warn_ip) as geo,
         count(1) as "登录次数"
         group by geo
         limit 10000
```

这里使用了另一个IP函数 `ip_to_geo` 来获得一个IP的所在经纬度，并获取前1万条。

> **说明** 了解基于IP的更多解析功能，例如获得IP所属运营商 `ip_to_provider` 、判断IP是内网还是外网 `ip_to_domain` 等，请参见IP函数。

1.5.2. 查看日志的时间分布

您可以在日志分析页面查看查询到的日志的时间分布柱状图。本文介绍如何查看日志的时间分布。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**调查响应 > 日志分析**。
3. 在**日志分析**页面查看日志的时间分布柱状图。

日志的时间分布柱状图展示了日志的分布时间和查询到的日志总数。横轴显示时间，纵轴表示查询的相关类型日志的条数。您可以根据需要进行以下操作。

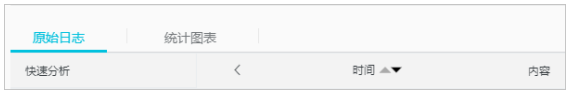
- 在日志时间分布图横轴上单击滑动以缩小选择的时间范围，并显示对应时间范围内的查询结果。
- 在页面右上角时间单击时间选择框，选择想要查看日志的时间段后，查看对应时间范围内的日志。

1.5.3. 查看原始日志

您可通过日志分析功能查看原始日志及其详细信息。原始日志支持下载到本地。

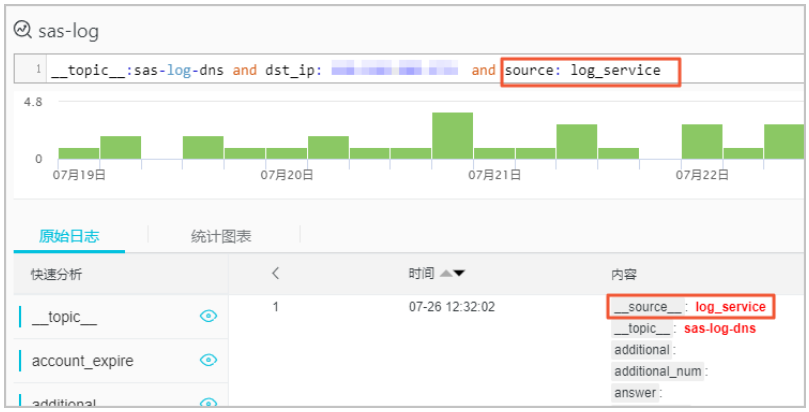
背景信息

原始日志页面展示了每一条日志的详细内容，包括时间、内容以及日志中的各个字段。各个日志字段的详细说明请参见日志字段说明。



操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**调查响应 > 日志分析**。
3. 在**原始日志**页签的**内容**栏中单击相应的字段，可将该字段自动加到搜索栏中。

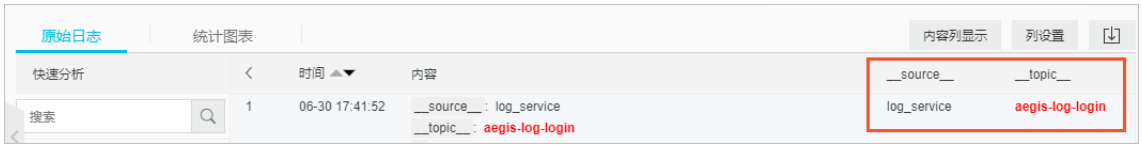


> **说明** 例如您选中并单击log_service字段后，搜索栏中将会加入该字段，单击**查询/分析**可以查看该字段相关的日志。

您可在**原始日志**页面进行以下操作：

- 单击**原始日志**列表右侧的**列设置**可将您需要的字段添加到原始日志列表中。

字段添加到**列设置**后，原始日志列表将以列的形式呈现该字段信息。



- 单击**列设置**右侧的 打开**下载日志**对话框。

在下载日志对话框中选择**直接下载**、**通过Cloud Shell下载**或**通过命令行工具下载**，单击**确定**下载日志。

- **直接下载**：以CSV格式将本页面的日志到本地。
- **通过Cloud Shell下载**：自动下载所有日志。详细操作指导请参见导出日志。
- **通过命令行工具下载**：使用命令行工具下载所有的日志。详细操作指导请参见导出日志。

1.5.4. 查看统计图表

日志分析服务支持图表形式展示日志分析结果。

您可以在控制台**统计图表**页面根据需要选择不同的图表类型、将日志统计图表添加到仪表盘或下载日志。

统计图表类型信息参见统计图表概述。

1.5.5. 快速分析

日志分析提供快速分析功能，为您提供一键交互式查询体验，帮助您快速分析某一字段在指定时间内的分布情况，提升检索关键数据的效率。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**调查响应 > 日志分析**。
3. 在**日志分析 > 原始日志**页签左侧的**快速分析**列表中，查看日志包含的字段以及对应的占比数据。

在**快速分析**列表中您可以根据需要进行以下操作。

- 单击指定日志字段右侧的图标 ，查看快速分析结果。
- 单击**快速分析**列右下角的图标 将分组统计的查询语句扩展到搜索框，便于进一步操作。同时，为您展示指定字段的日志统计图表内容。

1.5.6. 查询日志

云安全中心与日志服务打通，支持查询和分析您资产中的网络、主机、安全三大类共14种子类日志。云安全中心为您提供实时的日志自动采集、存储和基于日志服务的查询分析、报表报警、下游计算对接与投递的能力。

前提条件

已开通日志分析功能。具体操作，请参见开通日志分析。

版本限制说明

企业版和旗舰版支持14种子类日志，高级版仅支持主机和安全两大类共10种子类日志，免费版和防病毒版不支持日志分析功能。日志分析支持的版本信息详情，请参见功能特性。

操作步骤

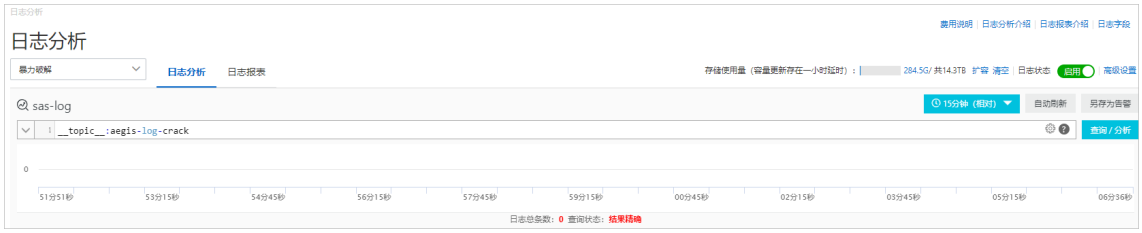
选择特定类型的日志，即可对采集到的日志数据进行实时查询与分析、查看或编辑仪表盘、设置监控告警等操作。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**调查响应 > 日志分析**。
3. 在**日志分析**页面左上角，选择您需要查看的日志类型，并将状态设置为**启用**。

4. 在**日志分析**页面，查询和分析日志。

   您可以进行以下操作：

   - **日志分析**页面展示您在步骤3中选择的日志类型的查询和分析结果，并且系统会为您自动匹配查询语句。



- 单击**查询/分析**按钮上方的时间，在**时间**面板设置需要查看的日志时间范围，然后单击**查询/分析**，可查看您所选时间范围内的日志信息。

> **说明** 云安全中心日志可保存180天，每条日志会在其日志时间的第180天被删除。

1.6. 日志报表仪表盘

云安全中心日志报表页面为您集中展示网络日志、主机日志、安全日志相关的仪表盘数据。

云安全中心日志分析功能开通后，系统为您自动创建报表仪表盘。您可以在云安全中心控制台**调查响应 > 日志分析**页面，单击**日志报表**页签，查看日志报表仪表盘。

日志类型	提供的日志报表
网络日志	DNS访问中心
	网络会话中心
	Web访问中心
主机日志	登录中心
	进程中心
	网络连接中心
安全日志	基线中心
	漏洞中心
	告警中心

网络日志

网络日志提供以下日志报表。

- DNS访问中心

  提供服务器上的DNS查询的全局视图，包括外网查询成功率、本地以及外网DNS查询的分布、趋势等。

图表名称	图表类型	默认时间范围	描述	样例
外网DNS流量包	单值比较	今天（整点时间）/同比昨日	外网DNS流量包数，以及与昨日同时段相比增加或减少的情况。	10.0个，0.01%
外网DNS请求成功率	单值比较	今天（整点时间）/环比昨日	外网DNS请求成功率，以及与昨日全天相比增加或减少的情况。	100%，0.01%

图表名称	图表类型	默认时间范围	描述	样例
独立DNS查询域名数	单值比较	今天（整点时间）/环比昨日	独立DNS查询域名数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%
内网DNS流量包	单值比较	今天（整点时间）/环比昨日	内网DNS流量包数，以及与昨日全天相比增加或减少的情况。	1.0千个，0.01%
外网查询设备分布	地图（全球）	今天（整点时间）	发生外网查询的外网设备数的地理分布。	无
外网DNS流量趋势	柱状图与线图	今天（整点时间）	每小时的外网查询的请求数以及成功率的趋势图。	无
内网DNS流量趋势	柱状图	今天（整点时间）	每小时的内网DNS查询的请求数的趋势图。	无
外网查询域名Top20	饼图	今天（整点时间）	外网查询数排名前20的域名。	无
内网DNS查询设备分布Top20	饼图	今天（整点时间）	内网查询数排名前20的设备实例。	无
内网查询域名Top20	饼图	今天（整点时间）	内网查询数排名前20的域名。	无

- 网络会话中心

  提供资产相关网络会话的全局视图，包括连接趋势与分布、连接目标以及接入的趋势与分布等。

图表名称	图表类型	默认时间范围	描述	样例
网络会话	单值比较	1小时（相对）/同比昨日	网络会话总数，以及与昨日同时段相比增加或减少的情况。	10.0个，-0.01%
独立目标IP	单值比较	今天（整点时间）/同比昨日	网络会话的**独立连接目标IP**的个数，以及与昨日全天相比增加或减少的情况。	10.0个，-0.01%
独立源IP	单值比较	今天（整点时间）/同比昨日	网络会话的**独立连接源IP**的个数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%

图表名称	图表类型	默认时间范围	描述	样例
独立目标端口	单值比较	今天（整点时间）/同比昨日	网络会话**独立目标端口**数，以及与昨日全天相比增加或减少的情况。	10.0个，-0.01%
网络连接趋势（协议）	流图	今天（整点时间）	每小时网络会话的各种协议（TCP、UDP等）的个数的趋势图，单位为个/每小时。	无
网络连接趋势（资产类型）	双线图	今天（整点时间）	每小时网络会话的资产类型（ECS、SLB等）的个数的趋势图，单位为个/每小时。	无
连接协议分布	饼图	今天（整点时间）	网络会话的连接协议（TCP、UDP等）的分布。	无
目标端口Top10	饼图	今天（整点时间）	网络会话中排名前10的目标端口的分布。	无
关联资产类型分布	饼图	本月（整点时间）	网络会话的关联资产类型（ECS、SLB等）的分布。	无
连接目标地址分布（世界）	地图（全球）	今天（整点时间）	网络会话的对外连接的目标的地理分布。	无
连接源地址分布（世界）	地图（全球）	今天（整点时间）	网络会话的接收连接的源目标的地理分布。	无
连接目标地址分布（中国）	地图（中国）	今天（整点时间）	网络会话的对外连接的目标的地理分布。	无
连接源地址分布（中国）	地图（中国）	今天（整点时间）	网络会话的接收连接的源目标的地理分布。	无

- Web访问中心

  提供主机对外HTTP以及基于主机的Web服务被访问的全局视图，请求成功率、访问趋势与有效率、被访问域名的分布以及其他相关分布等。

图表名称	图表类型	默认时间范围	描述	样例

图表名称	图表类型	默认时间范围	描述	样例
有效请求率	单值比较	今天（整点时间）/同比昨日	HTTP请求成功率（返回值<400的占比），以及与昨日全天相比增加或减少的情况。	0.01%，10.00
Web访问数	单值比较	今天（整点时间）/同比昨日	HTTP请求数，以及与昨日同时段相比增加或减少的情况。	1.0千个，-0.01%
独立访问目标数	单值比较	今天（整点时间）/同比昨日	HTTP请求独立目标数，以及与昨日全天相比增加或减少的情况。	10.0次，-0.01%
独立访问客户端数	单值比较	今天（整点时间）/同比昨日	HTTP请求独立源IP数，以及与昨日全天相比增加或减少的情况。	1.0千次，0.01%
访问趋势与有效率	柱状图与线图	今天（整点时间）	每小时的HTTP请求数以及成功率（返回值<400的占比）的趋势图。	无
独立访问目标/源IP趋势	双线图	今天（整点时间）	每小时的HTTP请求的独立源IP与目标IP数的趋势图。	无
访问状态分布	流图	今天（整点时间）	每小时的HTTP请求返回值（2xx、3xx等）的分布。	无
访问域名Top10	矩形图	今天（整点时间）	被访问排名前10的域名的分布。	无
请求内容类型分布Top10	饼图	今天（整点时间）	HTTP请求排名前10的内容类型（例如：text、plain）。	无
Referer	表格	今天（整点时间）	HTTP请求排名前20的Referer，包括URL、所在主机以及请求总数等。	无

主机日志

主机日志提供以下日志报表。

- 登录中心

云安全中心可展示主机登录中心仪表盘，为您提供主机上登录信息的全局视图，包括登录源和目标地址地理分布、趋势、登录端口和类型分布等。

图表名称	图表类型	默认时间范围	描述	样例
登录次数	单值比较	1小时（相对）/同比昨日	总的登录总数，以及与昨日同时段比的一个百分比增加减少状况。	10.0次，10%
被登录设备数	单值比较	今天（整点时间）/同比昨日	被登录的**独立主机设备**的个数，以及与昨日全天相比增加或减少的情况。	10个，-10%
独立登录源IP	单值比较	今天（整点时间）/同比昨日	登录设备的独立源IP个数，以及与昨日全天相比增加或减少的情况。	10个，10%
独立登录用户名	单值比较	今天（整点时间）/同比昨日	登录设备的独立用户名的个数，以及与昨日全天相比增加或减少的情况。	10个，10%
终端登录监控趋势	柱状图与线图	今天（整点时间）	每小时的发生登录事件的设备以及登录次数的趋势图。	无
登录方式趋势	流图	今天（整点时间）	每小时的登录方式（RDP、SSH等）的趋势图，单位为次/每小时。	无
登录方式分布	饼图	4小时（相对）	登录方式（RDP、SSH等）的趋势图的分布。	无
设备分布	地图（全球）	4小时（相对）	有外网地址的设备上发生登录的设备数的地理分布。	无
登录来源分布	地图（全球）	4小时（相对）	有外网地址的设备上登录来源的登录数地理分布。	无
独立登录源分布	地图（全球）	4小时（相对）	有外网地址的设备上独立登录来源数的地理分布。	无
登录最多的10个用户	饼图	4小时（相对）	登录次数排名前10的用户名。	无
登录最多的10个端口	饼图	4小时（相对）	登录次数排名前10的目标端口。	无

图表名称	图表类型	默认时间范围	描述	样例
激活用户列表	表格	4小时（相对）	在设备上可用的激活时间较早的30个账户。	无
登录机器最多30个用户和来源信息	表格	4小时（相对）	登录机器次数排名前30的用户和来源，包括来源网络、登录IP、用户名、登录方式、登录的独立设备数以及次数等。	无

- 进程中心

  云安全中心可展示主机进程中心仪表盘，为您提供主机上进程启动相关的全局视图，包括进程启动的趋势与分布、进程类型以及特定Bash或Java程序的启动分布等。

图表名称	图表类型	默认时间范围	描述	样例
进程启动次数	单值比较	1小时（相对）/同比昨日	进程启动事件总数，以及与昨日同时段比的一个百分比增加减少状况。	10.0千个，0.01%
相关设备数	单值比较	今天（整点时间）/同比昨日	发生进程启动事件的**独立主机设备**的个数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%
独立启动进程名数	单值比较	今天（整点时间）/同比昨日	启动的独立进程名的个数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%
终端设备数	柱状图与线图	今天（整点时间）	每小时的发生进程启动的设备以及独立进程名个数的趋势图，单位为个/小时。	无
进程启动趋势	线图	今天（整点时间）	每小时的每台设备平均启动进程数，单位为个/小时。	无
外网设备分布	地图（全球）	今天（整点时间）	发生进程启动的有外网地址的设备数的地理分布。	无
外网设备上进程启动次数分布	地图（全球）	今天（整点时间）	有外网地址的设备上发生的进程事件数的地理分布。	无

图表名称	图表类型	默认时间范围	描述	样例
启动次数最多的20个进程	表格	今天（整点时间）	启动次数排名前20的进程，包括进程名、进程路径、启动次数等。	无
触发Bash最多的前20个进程	表格	今天（整点时间）	触发Bash排名前20的进程，包括父进程名、触发总数等。	无
启动进程最多的前30个Java文件	表格	今天（整点时间）	启动进程次数排名前30的Java文件，包括Jar文件名、Jar文件路径、总的启动次数等。	无
启动进程最多的前30个客户端	表格	今天（整点时间）	启动进程次数排名前30的客户端，包括客户端、总的启动次数、这个客户端上启动次数最多的命令行、对应进程名、次数和占比等。	无

- 网络连接中心

  云安全中心可展示主机网络连接中心仪表盘，为您提供主机上网络连接变化的全局视图，包括连接的趋势与分布、连接目标以及接入的趋势与分布等。

图表名称	图表类型	默认时间范围	描述	样例
连接事件	单值比较	1小时（相对）/同比昨日	设备上网络连接的变化事件总数，以及与昨日同时段比的一个百分比增加减少状况。	10.0个，-0.01%
相关设备	单值比较	今天（整点时间）/环比昨日	发生连接变化事件的**独立主机设备**的个数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%
独立进程	单值比较	今天（整点时间）/同比昨日	发生网络连接的变化事件**独立进程名**数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%

图表名称	图表类型	默认时间范围	描述	样例
独立源IP	单值比较	今天（整点时间）/同比昨日	发生网络连接的变化事件的**独立连接源IP**的个数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%
独立目标IP	单值比较	今天（整点时间）/同比昨日	发生网络连接的变化事件的**独立连接目标IP**的个数，以及与昨日全天相比增加或减少的情况。	1.0千个，0.01%
网络连接趋势	双线图	1小时（相对）	每小时发生网络连接的设备数以及事件数的趋势图，单位为个/每小时。	无
连接类型趋势	双线图	1小时（相对）	每小时发生网络连接变化事件的连接类型（对外、接收）分布的趋势图，单位为个/每小时。	无
连接类型分布	饼图	1小时（相对）	网络连接变化事件的连接类型（对外、接收）的分布。	无
协议类型分布	饼图	1小时（相对）	网络连接变化事件的连接协议（TCP、UDP等）的分布。	无
外网设备分布	地图（全球）	1小时（相对）	发生网络连接变化事件的设备数的地理分布。	无
外网设备事件分布	地图（全球）	1小时（相对）	发生有外网地址的设备上网络连接变化事件数的地理分布。	无
对外连接目标分布	地图（全球）	1小时（相对）	网络连接变化事件的对外连接的目标的地理分布。	无
接收连接源分布	地图（全球）	1小时（相对）	网络连接变化事件的接收连接的源目标的地理分布。	无

图表名称	图表类型	默认时间范围	描述	样例
对外连接最多的30个设备	表格	1小时（相对）	发生对外连接类型的网络连接变化事件排名前30的设备，包括设备、对外连接事件数、独立的连接目标数以及样例。	无
接收连接最多的30个设备	表格	1小时（相对）	发生接收连接类型的网络连接变化事件排名前30的设备，包括设备、侦听IP、接收连接事件数、侦听端口数以及样例。	无
对外连接目标最多的30个设备	表格	1小时（相对）	发生对外连接类型的网络连接变化事件目标排名前30的设备，包括设备、对外连接事件数、独立的连接目标数以及样例。	无
接收连接最多的30个侦听端口	表格	1小时（相对）	发生接收连接类型的网络连接变化事件排名前30的侦听端口，包括侦听端口、接收连接事件数以及样例。	无
对外连接最多的30个进程	表格	1小时（相对）	发生对外连接类型的网络连接变化事件排名前30的进程，包括进程名、对外连接事件数、相关设备数以及路径样例。	无
接收连接最多的30个进程	表格	1小时（相对）	发生接收连接类型的网络连接变化事件排名前30的进程，包括进程名、对外连接事件数、相关设备数以及路径样例。	无

安全日志

安全日志提供以下日志报表。

- 基线中心

  提供基线检查相关的全局视图，包括检查问题分布、新增或处理基线的趋势、状态等。

图表名称	图表类型	默认时间范围	描述	样例
相关客户端	单值比较	今天（整点时间）/同比昨日	发生基线问题的**独立主机设备**的个数，，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%
新增基线	单值比较	今天（整点时间）/同比昨日	新增基线事件数，以及与昨日全天相比增加或减少的情况。	10.0个，-0.01%
验证基线	单值比较	今天（整点时间）/同比昨日	验证基线事件数，以及与昨日全天相比增加或减少的情况。	10.0个，-0.01%
高优先级基线	单值比较	今天（整点时间）/环比昨日	发生的高优先级的基线事件的个数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%
基线操作趋势	流图	今天（整点时间）	每小时的各种基线操作（新增、验证等）的趋势图，单位为个。	无
基线子类型趋势	流图	今天（整点时间）	每小时的各种基线子类型（系统账户安全、注册表等）的趋势图，单位为个。	无
基线状态趋势	流图	今天（整点时间）	每小时的各种基线状态（未修复、已修复）的趋势图，单位为个。	无
基线操作方式分布	环图	今天（整点时间）	各种基线操作（新增、验证等）的分布。	无
基线子类型分布	环图	今天（整点时间）	各种基线子类型（系统账户安全、注册表等）的分布。	无

图表名称	图表类型	默认时间范围	描述	样例
基线状态分布	环图	今天（整点时间）	各种基线最新状态（未修复、已修复、修复失败等）的分布。 注意 如果一台机器的一个基线有多个状态变化，取最新的状态归类。	无
新增基线Top10	环图	今天（整点时间）	在各个设备上新增次数排名前10的基线。	无
验证基线Top10	环图	今天（整点时间）	在各个设备上验证次数排名前10的基线。	无
基线事件客户端Top20	表格	今天（整点时间）	存在基线事件的数量排名前10的设备，包括客户端、基线事件数、新增基线数量、处理基线数量、高或中优先级数量。	无

- 漏洞中心

  提供漏洞相关的全局视图，包括漏洞分布、新增、验证、修复漏洞的趋势、漏洞状态等。

图表名称	图表类型	默认时间范围	描述	样例
相关客户端	单值比较	今天（整点时间）/同比昨日	发生漏洞问题的**独立主机设备**的个数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%
新增漏洞	单值比较	今天（整点时间）/同比昨日	新增安全漏洞事件数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%
验证漏洞	单值比较	今天（整点时间）/同比昨日	验证安全漏洞事件数，以及与昨日全天相比增加或减少的情况。	10.0个，-0.01%

图表名称	图表类型	默认时间范围	描述	样例
修复漏洞	单值比较	今天（整点时间）/同比昨日	修复安全漏洞事件数，以及与昨日全天相比增加或减少的情况。	10.0个，-0.01%
漏洞操作趋势	流图	今天（整点时间）	每小时的各种漏洞操作（新增、验证等）的趋势图，单位为个。	无
漏洞类型趋势	流图	今天（整点时间）	每小时的各种漏洞类型（Windows漏洞、Linux漏洞、Web-CMS漏洞等）的趋势图，单位为个。	无
漏洞状态趋势	流图	今天（整点时间）	每小时的各种漏洞状态（未修复、已修复）的趋势图，单位为个。	无
漏洞操作方式分布	环图	今天（整点时间）	各种漏洞操作（新增、验证等）的分布。	无
漏洞类型分布	环图	今天（整点时间）	各种漏洞类型（Windows漏洞、Linux漏洞、Web漏洞等）的分布。	无
漏洞状态分布	环图	今天（整点时间）	各种漏洞最新状态（未修复、已修复、修复失败等）的分布。 注意 如果一台机器的一个漏洞有多个状态变化，取最新的状态归类。	无
新增漏洞Top10	环图	今天（整点时间）	在各个设备上新增数量排名前10的漏洞。	无

图表名称	图表类型	默认时间范围	描述	样例
验证漏洞Top10	环图	今天（整点时间）	在各个设备上验证数量排名前10的漏洞。	无
修复漏洞Top10	环图	今天（整点时间）	在各个设备上修复数量排名前10的漏洞。	无
漏洞事件客户端Top20	表格	今天（整点时间）	存在漏洞数量排名前20的设备，包括客户端、漏洞事件总数、新增漏洞数量、验证漏洞数量、修复漏洞数量、各种类型漏洞数量。	无

- 告警中心

  提供安全告警相关的全局视图，包括新增或处理告警的趋势、分布与状态等。

图表名称	图表类型	默认时间范围	描述	样例
相关客户端	单值比较	今天（整点时间）/同比昨日	发生安全告警问题的**独立主机设备**的个数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%
新增告警	单值比较	今天（整点时间）/同比昨日	新增安全告警事件数，以及与昨日全天相比增加或减少的情况。	10.0个，-0.01%
处理告警	单值比较	今天（整点时间）/同比昨日	处理安全告警事件数，以及与昨日全天相比增加或减少的情况。	10.0个，0.01%
高优先级告警	单值比较	今天（整点时间）/环比昨日	发生的严重的安全告警事件的个数，以及与昨日全天相比增加或减少的情况。	10.0个，-0.01%
告警操作趋势	流图	今天（整点时间）	每小时的各种告警操作（新增、处理等）的趋势图，单位为个。	无

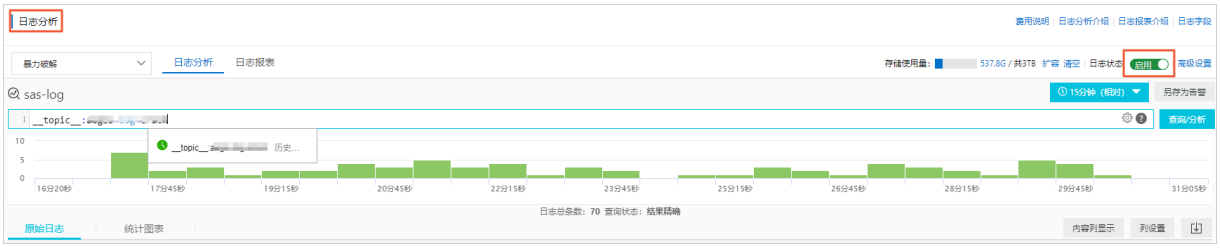
图表名称	图表类型	默认时间范围	描述	样例
告警级别趋势	流图	今天（整点时间）	每小时的各种告警级别（严重、可疑、提醒等）的趋势图，单位为个。	无
告警状态趋势	流图	今天（整点时间）	每小时的各种告警状态（未修复、已修复）的趋势图，单位为个。	无
告警操作方式分布	环图	今天（整点时间）	各种告警操作（新增、处理等）的分布。	无
告警级别分布	环图	今天（整点时间）	各种告警级别（严重、可疑、提醒等）的分布。	无
告警状态分布	环图	今天（整点时间）	各种告警最新状态（未修复、已修复、修复失败等）的分布。 注意 如果一台机器的一个告警有多个状态变化，取最新的状态归类。	无
新增告警Top10	环图	今天（整点时间）	在各个设备上新增数量排名前10的告警。	无
处理告警Top10	环图	今天（整点时间）	在各个设备上处理数量排名前10的告警。	无
告警事件客户端Top20	表格	今天（整点时间）	告警事件数量排名前20的设备，包括客户端、告警事件数、新增或处理事件数、严重或可疑事件数、告警种类等。	无

1.7. 查看日志报表

云安全中心**日志报表**页面展示了日志服务默认的**仪表盘**界面。您可以在当前仪表盘通过修改时间范围、订阅日志报表、设置刷新等操作，查看多种筛选条件下的仪表盘数据。

前提条件

日志分析页面右侧的日志状态为**启用**。日志状态为关闭时您将无法查看日志报表。



背景信息

日志报表页面提供以下三类共9个默认的仪表盘：

- 安全
  - 告警中心
  - 漏洞中心
  - 基线中心
- 主机
  - 登录中心
  - 进程中心
  - 网络连接中心
- 网络
  - DNS访问中心
  - Web访问中心
  - 网络会话中心

仪表盘各模块说明请参见日志报表仪表盘。

操作步骤

您可以参考以下步骤查看日志报表相关信息。

1. 登录云安全中心控制台。
2. 单击左侧导航栏**调查响应 > 日志分析**。
3. 在**日志分析**页面，单击**日志报表**页签，并选择主机日志的任一类型，例如选择**主机日志 > 暴力破解**，进入主机日志报表页面。

4. 单击**登录中心**、**进程中心**或**网络连接中心**，打开对应的日志报表页面。

5. 单击**登录中心**、**进程中心**或**网络连接中心**右上角的**请选择**，打开**时间**设置对话框。

6. 在**时间**设置对话框中选择您需要的配置，并单击**确定**。可选择相对时间、整点时间或设置自定义时间。

说明

- 设置时间范围后，该页面所有的仪表盘都将显示该时间范围内的数据。
- 时间选择器仅在当前页面临时生效，系统不保存该设置。您下次重新打开该报表页面时，仪表盘将恢复到默认时间范围。

7. （可选）单击**登录中心**、**进程中心**或**网络连接中心**右上角的**订阅**，在**新建订阅**页添加相应日志类型报表的订阅。
   i. 在**订阅配置**页签，配置订阅名称、频率等参数。

您可以参考以下说明配置订阅相关参数：

- **订阅名称**：待订阅的日志报表名称。系统根据日志类型，显示默认设置，您可以修改为自定义的名称。
- **频率**：待订阅日志报表发送通知的时间。
  - **每小时**：每小时整点时刻。
  - **每天**：每天的一个整点（00:00~23:00）时刻。
  - **每周**：可选择**周一**、**周二**、**周三**、**周四**、**周五**、**周六**或**周日**的一个整点（00:00~23:00）时刻。
  - **固定间隔**：每隔几天或几小时。
  - **Cron**：以表达式自定义时间。Cron表达式的最小精度为分钟，格式为24小时制。您可根据界面举例自定义频率。
- **添加水印**：开启后，图片自动加上通知渠道地址（邮箱或WebHook地址）。

ii. 单击**下一步**，设置通知类型。

您可以选择以下通知类型：

- **邮件**：添加收件人邮箱地址，支持添加多个收件人。
- **WebHook-钉钉机器人**：添加WebHook请求地址。地址获取方法请参考配置钉钉机器人通知。

iii. 单击**提交**，完成订阅添加。

8. （可选）您可单击**登录中心**、**进程中心**或**网络连接中心**右上角的**刷新**，设置日志报表刷新频率。

您可以设置以下刷新频率：

- **仅一次**：立即刷新。
- **自动刷新**：设置刷新频率。每15秒、60秒、5分钟或15分钟刷新一次。

1.8. 导出日志

云安全中心日志分析服务支持导出日志到本地，即支持下载本页日志（CSV格式）或全部日志（TXT格式）到本地。本文介绍了导出日志的具体操作。

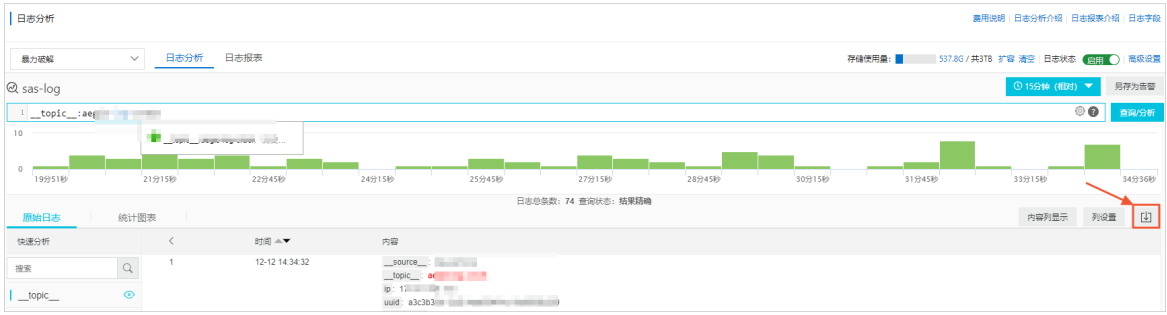
操作步骤

1. 登录云安全中心控制台。

2. 在左侧导航栏，单击**调查响应 > 日志分析**。
3. 单击**原始日志**列表右侧的下载日志按钮

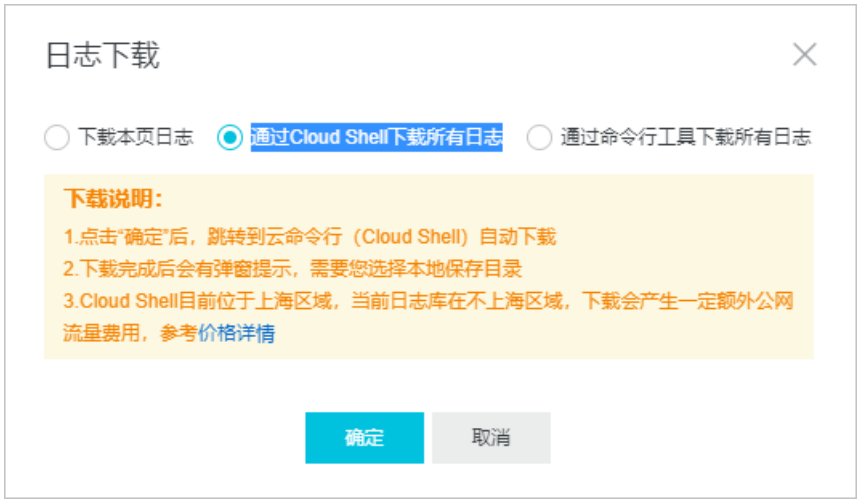
   打开**日志下载**对话框。

4. 在**日志下载**对话框中选择日志下载方式并保存日志。
   - 选择**下载本页日志**，并单击**确定**。

     云安全中心本页面的日志（CSV格式）会保存到本地。
   - 选择**通过Cloud Shell下载所有日志**下载所有日志。

     a. 单击**确定**跳转至Cloud Shell命令页面。
     b. 根据页面弹出的提示框要求，输入相关信息。
     c. 选择并确定日志文件保存到本地的路径。

     云安全中心的全部日志（TXT格式）会保存到本地。

> **说明** Cloud Shell目前位于上海区域，当前日志库如果不在上海区域，日志的下载会产生一定的公网流量费用。单击**价格详情**了解流量费用。

- 选择**通过命令行工具下载所有日志**下载所有日志。

a. 单击下载日志对话框中的**帮助文档**，打开命令行工具安装说明页面。

b. 安装命令行工具。

c. 单击**安全信息管理**，查看并复制当前用户的密钥ID和KEY。

d. 单击**复制命令行**并用当前用户的密钥ID和KEY替换该命令行中`【步骤2中的密钥ID】`和`【步骤2中的密钥Key】`。

e. 在CLI命令行工具中执行该命令。

命令执行后，云安全中心全部日志将自动下载并保存到运行命令的当前目录下的download_data.txt文件中。

1.9. 高级设置

云安全中心日志分析服务提供高级设置功能，您可通过高级设置功能跳转到日志服务页面，执行告警与通知、实时订阅与消费、数据投递和对接其他可视化等高级操作。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**调查响应 > 日志分析**。
3. 单击**日志分析**页面右上角的**高级设置**按钮。

4. 在高级设置对话框中单击**前往**，打开日志服务控制台。
5. 在日志服务管理控制台根据您的需要执行更多操作。

   日志服务的相关操作请参见以下文档。

   - 设置告警
   - 通知方式
   - 数据投递

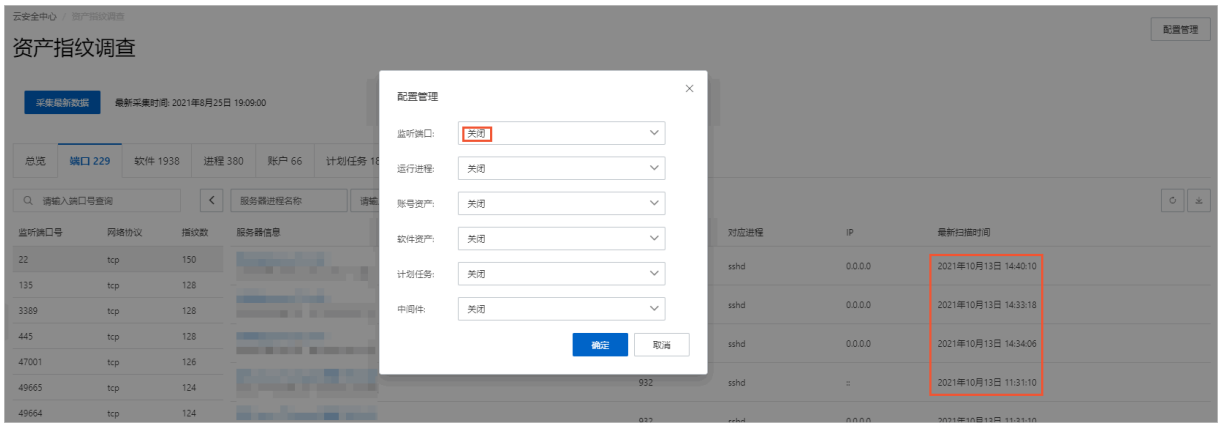
   > **说明** 除了通过管理控制台进行操作外，日志服务还提供了API方式写入、查询日志数据、管理您的项目及日志库等功能。有关日志服务API的详细内容，请参见日志服务APIAPI概览。

2.常见问题

本文汇总了调查响应功能的常见问题。

资产指纹调查的资产指纹采集频率为关闭状态，为何查看最新扫描时间还在扫描？

如下图所示，资产指纹调查的**配置管理**对话框中的资产指纹采集频率为**关闭**状态，为何查看**最新扫描时间**还在扫描？



资产指纹调查的**配置管理**对话框中相关的资产指纹采集频率为**关闭**状态时，页面上最新扫描时间的刷新变化是因为您开通了日志服务。开通日志服务后，云安全中心会采集这些数据用于日志分析，因此在该资产指纹页签下，仍会看到最新扫描时间的变化。

为什么在资产指纹页面看不到任何数据

开通云安全中心企业版或旗舰版后，云安全中心不会自动采集资产指纹数据。因此在您未进行资产指纹数据采集前，资产指纹页面看不到数据。您需要配置自动周期性采集或手动立即采集来获取最新的资产指纹数据。具体操作，请参见资产指纹调查。