神州云科 Yunke China | DCN

DCSSA 系列日志审计系统

高性能的日志统一收集管理展示平台

产品概述

DCSSA 系列日志审计系统提供了众多基于日志分析的强大功能，如安全日志的集中采集、分析挖掘、合规审计、实时监控及安全告警等，系统配备了全球 IP 归属及地理位置信息数据，为安全事件的分析、溯源提供了有力支撑，该系统能够同时满足企业实际运维分析需求及审计合规需求，是企业日常信息安全工作的重要支撑平台。

产品图片

产品特点

安全审计

随着国家和各行业信息安全技术标准的不断出台和完善，对安全审计的要求逐步成为网络安全管理中的基本要求。

通常攻击者在攻击行为结束时都会清理受影响系统中的日志，以便清除攻击的痕迹。日志安全审计系统会实时采集各类网络设备、安全设备、操作系统和应用系统的日志信息，将日志以数据方式进行固化保存，即使被攻击系统的日志遭到清理也可提供完整的日志记录，为后续事件调查提供有力依据。

云科安全日志审计系统通过对异构网络环境下各系统日志信息的集中保存，能够很好的满足安全审计要求。同时依托于大数据分析和全文检索技术可以对海量数据进行任何关键字的检索，实现秒级呈现。同时可以在搜索结果基础上进行筛选、并通过可视化功能对筛选的内容实现进一步的关联，帮助用户高效的对海量数据进行挖掘和分析。

跨平台、跨系统多元异构日志采集

日志安全审计系统支持 Syslog、WMI、HTTP (HTTPS) 、TCP、UDP、WebSocket、JDBC 等多种数据采集方式，同时提供采集接口的定制开发。采集器可以完整的实现从终端到服务器、从设备到网络、从应用到业务的各种日志的全面采集，支持主流网络设备、安全设备、操作系统和应用系统的各种日志。

统一日志监控

日志安全审计系统将网络中部署的各类网络设备、安全设备、操作系统和应用系统的日志全部汇集起来，使得用户通过单一的管理控制台对网络中的安全事件进行统一的监控，不必反复在多个控制台软件之间来回切换即可全面掌控整个网络的安全事件情况，可以高效的对网络安全事件做出全面、准确的判断。

事件关联分析和实时告警

依托高性能非结化存储技术、全文索引技术和流引擎数据分析技术，云科安全日志审计系统对于整个系统的效率进行了从底到上全面的优化，通过规则关联、场景关联和行为关联等手段对事件日志进行关联分析，可以满足各类使用场景下对于审计实时告警的要求。针对各类日志审计要求提供丰富的告警策略，支持用户灵活定制，支持多种实时告警方式和同类告警的归并。

溯源分析

日志安全审计系统一方面对采集到的各类网络设备、安全设备、操作系统和应用系统的日志从时间、空间等多种维度进行深度关联分析和数据挖掘，梳理出安全事件发生的脉络和攻击的路径以及同类事件的影响域。

功能规格

功能分类	详细指标
部署模式	支持集中和分布式部署、集群部署、热扩容
支持性	系统满足设备的信息采集要求，主要包含各类主机、安全设备、网络设备、数据库、中间件等主流设备
	完整支持 IE11、Firefox、Chrome 等主流浏览器
资产管理	可以添加、修改、删除资产；对资产的基本属性进行维护；资产可以增加自定义属性
	资产支持组织管理、网络管理
	系统支持对 IP 对象的自动发现功能；对自动发现的设备可以转资产或删除
日志采集	支持 Syslog、Syslog-ng 、SNMP Trap、文件、WMI、SFTP、数据库 等方式采集日志
	被采设备无需安装任何代理
	日志采集器可实时或按设定的时间将指定的日志送到审计中心
	日志采集器在将日志送往审计中心的时候，可以制定传送策略，仅传送符合条件的日志
	支持多个日志采集器
标准化	对日志格式进行标准化操作时，将不破坏原始日志内容
	标准化自动识别系统类型至少达到 150 种
	系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段，日志清洗后的标准化字段粒度至少达到 90 个字段
	对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义
	系统的标准化策略具备良好的可扩展性，可通过配置文件或界面实现管理功能
	支持不同设备相同 IP 的日志识别
日志处理	可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间地占用
	系统具有归并技术，安全事件收集代理会在一段时间内比较收到的安全事件，如果安全事件相同，则只需发送一条安全事件，该安全事件应包括安全事件详情及该安全事件发生的次数，这样可以减少安全事件通信量

日志分析与审计	支持根据设备类型，按日期展示日志的接入情况，包含不同级别日志数量统计
	挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，系统提供了 GUI 方式的关联规则设置功能，关联的类型包括基于规则和基于统计的
	支持基于异常统计模型的检查分析功能，如：识别异常的流量攻击等
	若日志满足系统内置或用户定义的关联策略，将产生关联事件
	支持显示审计事件分类统计列表，根据审计策略名称、审计事件类型、被审计人员、目标设备地址四个维度展现
	支持以列表的方式展示告警、告警声音设置、告警过滤策略；支持系统支持通过 GUI 设置告警策略； 系统内置丰富关联/审计类告警策略，并灵活支持自定义策略。
用户管理	支持根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理

选配信息

项目	DCSSA-D60	DCSSA-D110	DCSSA-D220
机型	1U 可上架标准设备	1U 可上架标准设备	1U 可上架标准设备
网络接口	6 个千兆电口， 1 个 CON 口	6 个千兆电口， 1 个 CON 口	6 个千兆电口， 1 个 CON 口
存储空间	2T 硬盘存储	2T 硬盘存储	4T 硬盘存储
扩展插槽	2 个通用扩展插槽	2 个通用扩展插槽	2 个通用扩展插槽
尺寸	440mm（宽）*400mm（深）*44mm（高）	440mm(宽)*400mm(深)*44mm（高）	440mm(宽)*400mm(深)*44mm（高）
工作环境温度	0-45℃	0-45℃	0-45℃
工作环境湿度	10-95%(非凝结状态)	10-95%(非凝结状态)	10-95%(非凝结状态)