力控科技 FORCECON | HUACON 力控华康

华康日志
审计分析系统
HC-LAS

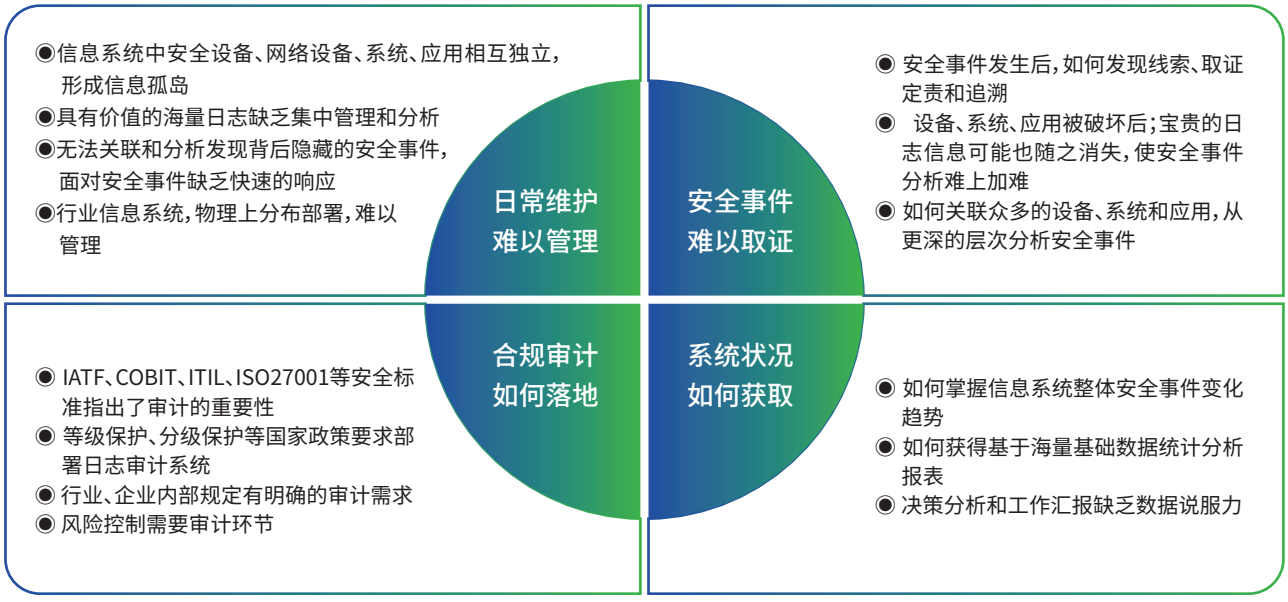
北京力控华康科技有限公司

www.sunwayland.com

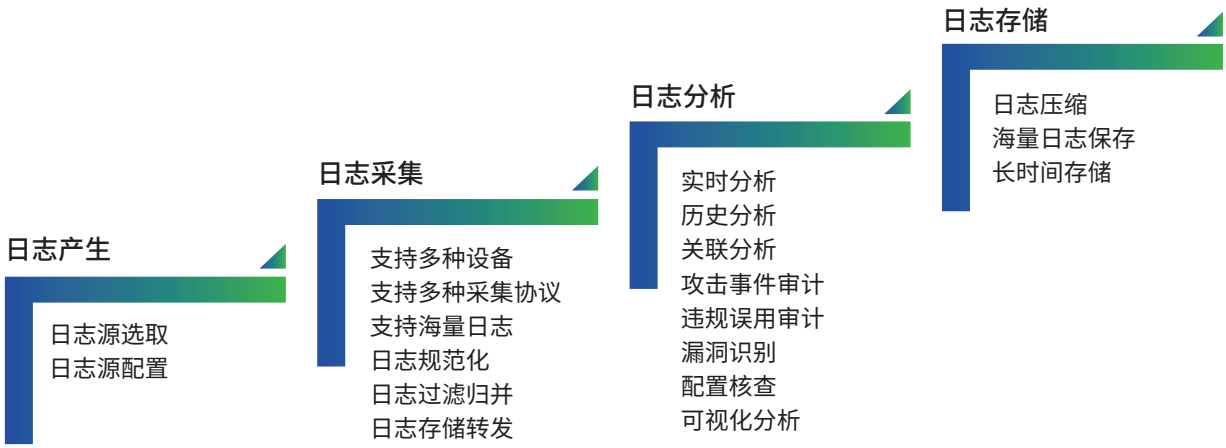
目 录

产品概述

现如今，每个用户网络包含大量的信息资产，包括各种网络设备、安全设备、主机、应用及数据库等，每种设备类型的日志格式都不相同，即使是记录同一事件，也都有各自的日志规格。例如同样的登录失败信息，防火墙中的描述和主机操作系统中的描述格式就可能根本不相同，这样会迫使审计人员去了解每种设备类型的格式。但是，每个产品的日志量是巨大的，例如一个标准的入侵检测系统每天可能产生超过千万数量的事件日志，海量的数据常常让运维审计工作变得没有毫无头绪，成为业务顺畅运行的挑战。



◉ 海量日志-无法有效管理
◉ 信息孤岛-日志无法关联
◉ 大量误报-关键告警淹没
◉ 多种界面-高成本低效率
◉ 法律法规-网络安全法规定日志留存不少于六个月
◉ 安全分析-日志单独查看无法发现问题，需结合其他相关的日志分析，才可能发现潜在的攻击威胁



产品架构

分层设计

采用分层的数据处理结构设计，从数据采集到最终的数据分析呈现形成完整的处理逻辑过程。

◉ **采集层**

采集数据来源包括网络设备、安全设备、数据库、中间件、主机等。该层提供多种接口进日志的采集和对接，支持Http、Syslog、Snmptrap、Tcp、Vflow、WMI、FTP、SFTP、SSH、TELNET、SCP、LEA、FILE、WebService、AGENT等方式采集。

◉ **数据层**

对采集的数据进行预处理，包括数据清洗、数据归并、数据富化，最终数据转换为平台可理解的格式化数据，以文件的形式进行存在，等待分析。

◉ **分析层**

读取经过预处理后的数据进行离线计算和实时机算。再次此进行数据的检测、分析和统计，同时，内置的多条安全关联规则可将数据进行归并告警。

◉ **表示层**

基于APP的方式设计整个数据可视化的展示，基于从数据存储系统中获取数据的接口，读取展示数据，提供各种数据的安全可视服务及对外接口服务。

大数据架构

整体设计框架具备如下大数据特性：

◉ **采用大数据技术架构**

1）使用流处理框架来进行并行处理，具备可靠性和容错性，同时为海量数据集分析提供支撑。

2）使用自主研发的分布式存储引擎为基础元数据、分析数据、分析结果提供了快速检索能力。

◉ **智能分析技术支撑**

内置了MLib等库，可用于机器学习（如聚类、分类算法）、关联分析等的使用。目前已经在系统中使用了机器学习、EBA基线分析等技术。

同时，基于APP设计的智能分析引擎可通过在线、离线升级的方式，快速更新现有检测能力、持续集成新的检测技术。

◉ **高性能分析能力**

单台设备每天达亿级实时日志分析，约合3TB数据。

产品组件

◉ **采集器**

主要实现日志采集、日志解析与格式统一、日志预处理、完成日志向平台的传送等功能，被监控设备分为标准设备（支持Syslog或SNMP trap）和非标设备（不支持Syslog和SNMP trap）；采集器主要完成标准设备日志的收集功能。把采集的日志数据过滤并转化为统一定义的标准数据格式；完成日志压缩和归并。

◉ **通信服务器**

通信服务器完成采集器与平台间的通信，将格式统一后的日志直接写入数据库并且同时提交给关联分析模块进行分析处理。通信服务器可以接收多个采集器的日志；在平台尚未支持统一日志格式时，能够根据要求，将定义的统一日志转换为所需要的日志格式。

◉ **关联分析**

对于整个日志平台收集到的事件种类多，数量大，为了更有效地对这些海量的事件进行分析和处理，确保第一时间对各种存在的安全问题采取措施，平台必须具有强大的事件处理和分析功能。目前对实践进行处理和分析最有效的方法就是做事件的关联。包括实时进行关联分析、跨设备关联分析、基于事件因果关系、事件安全要素、跨协议层、多层架构、时间回溯以及关联结果的回放等内容。

◉ **采集代理Agent**

Agent主要完成非标准设备（不支持Syslog和SNMP trap）的安全日志采集，Agent采集到日志信息后，通过SYSLOG日志发送给采集器。主要包括文件型Agent、数据库型Agent、Api型Agent的开发工作，至少支持windows主机日志及性能采集；支持通过SNMP Get方式对主流安全设备、网络设备的性能数据采集；IIS、Apache web服务器日志收集；Mysql、SQL server数据库日志采集。

产品特点

日志产生
- 日志源选取
- 日志源配置

日志采集
- 支持多种设备
- 支持多种采集协议
- 支持海量日志
- 日志规范化
- 日志过滤归并
- 日志存储转发

日志分析
- 实时分析
- 历史分析
- 关联分析
- 攻击事件审计
- 违规误用审计
- 漏洞识别
- 配置核查
- 可视化分析

日志存储
- 日志压缩
- 海量日志保存
- 长时间存储

高性能的日志管理技术架构

为了应对海量日志管理带来的挑战，华康日志审计分析系统采用了国内领先的高性能日志采集、分析与存储架构，系统性的设计产品架构，真正使得华康日志审计分析系统产品成为一款能够支撑持续海量日志管理的系统。

全面智能的日志采集能力

全面的采集方式支持，包括：Http、Syslog、Snmptrap、Tcp、Vflow、WMI、FTP、SFTP、SSH、TELNET、SCP、LEA、FILE、WebService、AGENT等，满足不同采集需求。

实时的连接检查和完整性检查以及可自定义的缓存功能，可确保平台接收到所有数据，并对传输链的各个环节进行监控。

通过配置过滤和聚合功能可以消除无关数据，合并重复的设备日志，强大的数据压缩功能可节省昂贵的带宽。

详尽的日志范式化和日志分类

日志处理系统能够根据配置的规则抽取日志关键字段，将非结构化的日志通过范式化处理后，转换成结构化数据。通过抽取关键字段，一方面系统可以对关键字段进行统计分析，另一方面审计人员不必再去熟悉不同厂商不同的日志信息，从而大大提升审计工作效率。系统对关键字段及原始日志进行索引，用户可对关键字段及原始日志进行搜索。

系统已经内置了常见日志的解析规则，对于没有预先配置解析规则的日志，用户可通过管理界面配置解析规则或者导入解析规则，抽取关键字段。即使没有抽取关键字段，用户仍然可以通过全文检索搜索日志。

系统支持对各种安全事件日志（攻击、入侵、异常）、各种行为事件日志（内控、违规）、各种弱点扫描日志（弱点、漏洞）、各种状态监控日志（可用性、性能、状态）等进行范式化处理。

创新的日志解析能力

创新引入了解析规则激活技术，仅当接收到对应的日志后，规则才会被激活，同时支持未识别日志标识处理，采用多级解析功能和动态规划算法，实现灵活的未解析日志事件处理，同时支持多种解析方法（如正则表达式、分隔符、MIB信息映射配置等），日志解析性能与接入的日志设备数量无关。

创新引入基于机器学习的智能化日志解析识别技术，在简化配置人员规则配置工作的同时，更进一步提高日志解析准确率。

智能关联事件分析

华康日志审计分析系统，对于采集并范式化后的的事件，通过内置关联模型，能基于事件的时序性、因果关系、相关安全日志和脆弱性等进行关联分析，形成具有承上启下的安全事件关联集，并围绕事件的证据链视角进行呈现和告警。如根据主机遭受RDP暴力破解后，出现永恒之蓝内网传播，来告警可能中了Globeimposter勒索病毒；或发现内网某服务器遭受永恒之蓝攻击，能关联该服务器是否存在永恒之蓝漏洞，来及时预警。

关联引擎采取了基于内存的实时关联分析的设计，全内存运算方式保证了事件分析极高的效率和实时性。

另外，在关联算法方面，华康日志审计分析系统有如下优势：

◉ 标准化之上的关联规则，适应性强。

◉ 可定制性强，几乎可根据通用事件的任何字段进行关联，可自定义和导入关联规则。

◉ 基于逻辑表达式，可以进行复杂关联。

◉ 时序宽容，无惧乱序。

分级部署能力

华康日志审计分析系统能够支持单节点部署和多节点分级部署，同样适用于大型企业和组织具备多层级组织机构的环境，也能满足需要单独部署在逻辑隔离域进行日志收集的需求，通过分级部署能力，用户可以轻松的在同一系统中查询不同下级节点的日志，减轻审计管理员的工作压力，提高日志审计效率。

另外基于SSL加密通讯技术，使跨互联网部署成为了可能，异地监控不再需要昂贵的专线私网模式。可以适用于从大型电信级网络环境到寥寥数台设备的中小企业。

自进化智能分析引擎

基于华康自研“自进化”智能分析引擎，结合多种机器学习算法（如聚类、分类、回归、关联规则等）在TB级的数据中快速实现有用数据提取、数据关联分析、时间预测以及未知威胁发现等相关分析，使得日志分析速率和准确性大幅度提升。并将独立的智能分析模型进行聚合调优、更新和分发，构建自进化智能分析引擎。

同时，分布式智能分析引擎将系统分析感知能力前移，实现多节点探针智能分析模型的持续优化，大幅度提高系统的日志分析能力；并通过智能分析能力下沉到末端采集器，大幅降低系统分析日志的处理成本，为整个网络系统贡献了“自我进化”和“降低建设成本”两大核心价值。

可视化的日志分析统计

事件可视化（Event Visualization）是指日志审计分析系统以图形化的方式将归一化和关联分析后的事件及其事件之间的关系形象展示出来的过程，反映出大量事件之间的相互作用关系。事件可视化是实时的将安全管理和运维人员从繁重的事件查看工作中解脱出来，实现安全运维人员从点到线，从线到面，站在全局视角去理解网络的安全状态，及时直观地进行时间调查，发现网络中隐藏的安全问题。具备强大的事件可视化能力，变用户日常安全管理的认知为感知。

合规性审计报表报告

内控与合规性审计越来越受到企业和相关监管部门的重视，法规遵从、企业内控成为IT业界的热点话题和发展趋势，通过对用户网络环境中安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统等日志进行全面分析与审计，集成各种合规性关键控制点需求，建立基于日志与行为分析的合规性安全审计平台，为用户提供合规性审计报表报告，充分满足各项标准、法规（萨班斯法案、等保要求、分保要求）的合规性控制需求，降低合规性成本。

可配置的规则和策略

华康日志审计分析系统采用了基础系统和业务规则分离的设计架构，将事件分析规则、关联分析规则、告警规则、综合报表规则等独立出来。各个部分可以独立演进、独立配置、独立升级，由华康公司多年安全经验的专门团队定制开发，这种模式具有非常强的反馈速度和适应性。

可维护性及可扩展性

华康日志审计分析系统具有对自身的维护配置功能，如：系统参数设置、系统日志管理等。硬件系统采用模块结构，保证系统内存、CPU及储存容量的扩展。硬件配置的升级不会引起软件的修改和开发，每个组件都可以横向扩展，通过增加设备满足业务需求。

面向服务的体系架构

系统基于J2EE的体系架构设计，层次化的逻辑处理技术，具有极高的可扩展性和稳定性。分层架构更好的支持多级分布式部署，能够灵活、无缝的扩展系统的容量，使得功能模块的管理信息集中在统一平台上发布和展示。通过开放、标准化、服务化的架构，让企业能够灵活方便地接入和开发第三方应用。

海量的日志处理能力

华康日志审计分析系统使用大数据技术，在并发内存处理机制方面能够带来数倍于其它采用磁盘访问方式的解决方案，借助离线计算引擎在小时级别内，即可完成对海量日志的处理。

灵活的扩展存储方案

华康日志审计分析系统提供了多种日志存储扩展方式，支持按需选择日志存储扩展方案，可支持《网络安全法》规定留存6个月日志的要求。

全面支持IPv6部署以及数据接入

华康日志审计分析系统支持IPv6的部署以及IPv6环境下的日志采集、分析以及检索查询。

过滤处理

采集器为了消除不必要的日志事件，或者去掉不重要的日志事件，可以设定过滤规则。

任何标准化完成后的通用事件，都会经过过滤规则匹配。

当满足匹配后，此事件就会被过滤，直接过滤掉，不会进入后续模块进行处理。

当不满足匹配，此事件就不会被过滤，直接进行后续模块处理。

日志采集

支持对各类网络设备、安全设备、操作系统、数据库、应用系统的日志、事件、告警信息进行全面的日志采集。处理的结果分享给网内其它控制中心和终端，以提高全网的安全防护能力，完成对一次攻击及其报警的闭环防御流程。

日志信息解析

接收到的原始日志信息，经过解析规则的模式匹配，提取出直接信息和非直接信息，最终就得到了解析后的通用事件。

日志信息解析模块启动的时候，需要首先进行规则库的加载，加载各种日志格式的解析、映射定义。加载完成后，才能进行日志的解析处理。

当原始日志无法匹配规则库中任何一个规则时，就会生成一个未识别日志信息。

用户收到未识别日志信息后可向厂家索取指导手册按手册说明进行规则添加，以支持这种日志格式，如存在很多类型的日志无法解析时，也可将收集到的原始日志反馈给厂家，由厂家适配后提供规则库升级包给用户，同时支持在线升级和离线升级两种形式。

日志信息标准化

完成解析后的通用事件，可以根据规则库，进行标准化处理。

标准化主要是对解析后的日志，根据标准化的通用事件格式，对各个标准化字段，进行信息的直接映射、非直接映射处理。

映射处理基于预先定义的标准。在本系统，标准基于对安全领域的技术、威胁、模式、以及网络层、应用层的抽象。

标准化过程，也会进行字段的格式处理，如时间戳的format、locale的处理。经过映射处理后，就得到了最终的通用事件。

日志资产管理

按照日志资产重要程度和管理域的方式组织日志资产，提供便捷的添加、修改、删除、查询与统计功能，支持日志资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需日志资产的信息，并对资产进行关键度赋值。

聚合处理

采集器为了减少重复日志事件的数量，会在处理流程中，通过设定一个聚合周期、聚合规则，对于在聚合周期内，所有满足聚合规则的事件，进行聚合处理，得到聚合事件。

聚合事件中的事件计数字段，会记录本次聚合的源事件的数量。聚合处理不会影响后续关联分析等处理。

日志缓存

为了实现日志缓存的需求，需要对队列进行持久化处理。采集器日志缓存基于状态驱动。当队列的空闲状态较低时，超过最低阈值后，会触发回写模块，把内存队列中的事件持久化到设备磁盘系统上。当队列的空闲状态较高时，超过最高阈值后，会触发加载模块，把磁盘系统上持久化的数据，加载到内存队列中。

状态检测处理

为了实现状态检测处理，需要维护每个资产的状态信息。当收到设备的原始日志后，会更新此设备的事件计数、最后活跃时间等信息。当状态检测周期到达后，采集器会把每个设备的状态信息组装成心跳事件，上送给上层设备。

通信服务器的功能

通信服务器接收各个采集器上发的通用事件，汇总后进行存储。

通信服务器处理收到的心跳事件，更新对应资产的心跳状态，并持久化心跳信息到数据库中。

通信服务器处理配置同步请求。当用户或管理员在界面上新增、删除、修改了客户、资产、规则库后，通信服务器应该能够把这些改动同步到各个连接的采集器上。

关联引擎的功能

关联引擎从接收到的通用事件中，基于关联规则，发现关联事件。

关联事件包括各个原始事件列表。

关联引擎产生的关联事件，能够支持入库接口，进行持久化处理。

关联引擎支持自定义的关联规则，支持规则的启用、禁用。

日志代理的功能

当某些设备设备无法主动发送SYSLOG日志、或者由于配置等原因(如不允许直接网络访问)的时候， 在目标对象主机上部署一个轻量级的Agent进程，用于主动抓取日志。

Agent采集到日志信息后，通过SYSLOG日志发送给采集器。

Agent支持以下的日志获取方式：

◉ 通过读取日志信息。

◉ 通过Windows日志API接口获取日志信息。

◉ 对系统可用性资源(如CPU、内存、磁盘、任务)进行监控。

统计报表

提供丰富的报表管理功能，预定义了针对各类服务器、网络设备、防火墙、入侵检测系统、防病毒系统、终端安全管理系统、数据库、策略变更、流量，设备事件趋势以及总体报表，满足等保等其他合规性要求，提供自定义报表，用户可根据自身需要进行定制。

日志备份归档

支持按照日志存储周期进行备份，当磁盘空间日志存储量达到一定百分比时可设定为删除磁盘中的历史日志，并进行告警；手动备份和恢复时，可以显示恢复和备份的进度。

Web服务

WEB服务提供日志展现、数据可视化，支持各种统计功能及图表展现，实现流畅的图形用户交互。展示时间折线图、条形图、饼状图等，让数据分析更直观。

典型应用

单机部署

适用于小型企业网络环境：

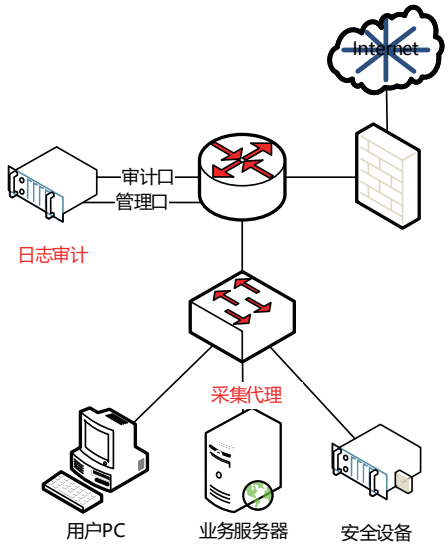
◉ 无需更改现有网络结构。

◉ 日志接入不影响当前业务。

◉ 日志接入采用syslog、SNMP、JDBC/ODBC等标准协议/接口。

◉ 支持采集代理Agent接。

单设备部署模式适用于网络结构简单的环境，日志审计产品采用旁路部署即可，与资产之间网络可达即可。网络设备通过syslog等协议发送日志到日志审计平台，业务服务器资产需要安装采集代理，通过采集代理采集日志后发送到日志审计平台。



分级部署

◉ 大型电信级网络环境；

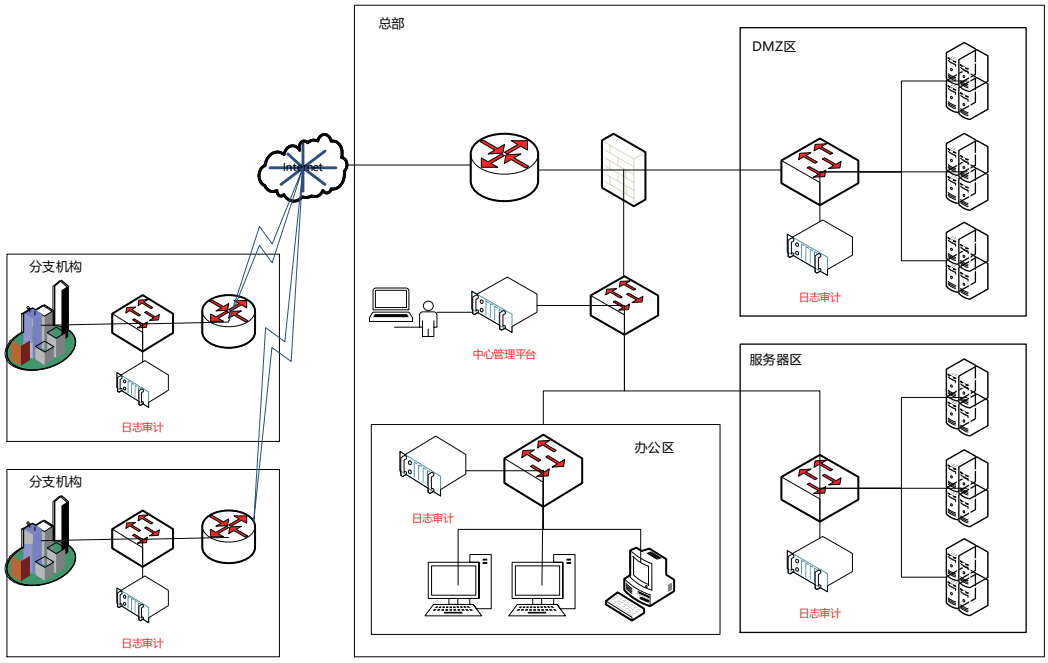
◉ 集中管理，所有配置管理统一入库；

◉ 日志事件分散解析、关联分析，集中存储、查询；

◉ 管理中心集中存储解析、关联分析后的核心关键数据，降低数据中心压力；

分级部署模式适用于网络节点众多，网络结构复杂，数据流量大，单台日志审计设备难以满足审计能力需求的场景。

分级部署模式下，采用中心管理平台+采集器的模式进行部署，在中心管理平台进行集中管理。在互联网出口交换机、内网交换机、DMZ区交换机、服务器区交换机、各分支机构交换机分别部署日志审计设备作为采集器，然后在总部部署一台日志审计设备作为中心管理平台，形成全网审计能力。



力控科技 FORCECON

北京力控华康科技有限公司

地址：北京市海淀区天秀路10号中国农大国际创业园1号楼
总机：010-62839678
全国统一服务热线：400 650 1353
www.huacon.com.cn

关注公众号　关注小程序