聚铭睿合管控巡航平台

产品白皮书

聚铭网络科技有限公司

2024 年 04 月

目录

声明 1

联系信息 2

1. 需求背景 3

2. 现状和挑战 3

3. 设备集中管控的未来趋势 3

4. 主要功能简介 4

4.1. IT 设备集中运维 4

4.1.1. 设备状态集中监控 4

4.1.2. 业务集中监控 4

4.1.3. 设备告警管理 5

4.1.4. 自动运维巡检 5

4.1.5. 运维编排 6

4.1.6. 设备日志收集 6

4.2. 资产管理 7

4.2.1. 资产台账 7

4.2.2. 拓扑管理 8

4.3. 运营仪表板 9

4.4. 工单管理 10

4.5. 个人工作台 10

4.6. 报表管理 10

4.7. 知识库管理.....11
4.8. 系统管理.....12
5. 产品优势.....12

声明

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司和北京聚铭信安科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

北京总部：北京市海淀区丹棱街 18 号创富大厦 9 层

南京总部：南京市雨花台区软件大道 180 号南京大数据产业基地 7 栋 4 层

电　　话：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

聚铭网络技术服务以及营销网络覆盖全国，并在各地设有办事处和分支机构，为客户提供无微不至的解决方案和高效的服务支持。聚铭专家团队 7x24 小时全天候在线，确保在安全事件发生时提供分钟级应急响应。

1. 需求背景

随着企业业务的快速发展，IT 设备数量不断增加，设备类型也日益多样化。传统的 IT 设备管理方式已经无法满足现代企业的需求，面临着许多挑战，如设备管理效率低下、安全性问题突出、无法实现自动化配置等。因此，实现 IT 设备的集中管控已经成为企业 IT 部门的迫切需求。

2. 现状和挑战

1. 设备数量和种类众多：随着企业的发展和信息化程度的提升，IT 设备数量和种类日益增多，包括服务器、网络设备、存储设备、安全设备等，每种设备的性能、品牌、型号都存在差异。

2. 设备管理效率低下：传统的 IT 设备管理方式通常采用手动方式，效率低下，容易出错，而且缺乏统一的监控管理平台，无法对设备进行实时监控和预警。

3. 故障排除时间过长：当 IT 设备出现故障时，可能需要花费大量的时间进行故障排除，这可能会对企业的业务连续性造成影响。

4. 缺乏统一的运维流程：没有统一的运维流程，每个设备可能都有自己的运维方式和方法，这可能会导致运维效率低下，也可能会导致运维成本高昂。

5. 缺乏统一的运营管理平台：信息化建设的 IT 设备需要进行统一的管理，包括监控、告警、维护等方面，以提高管理效率和质量。

因此，IT 设备集中管控的需求越来越强烈，需要一个集中管控平台来满足这些需求。这个平台应该能够集中管理设备的性能、状态、业务等信息，能够实时监控设备的运行状态，能够及时发现和预警故障，能够快速定位和解决故障，从而提高运维效率和质量，降低运维成本。

3. 设备集中管控的未来趋势

未来，随着物联网、人工智能和自动化等技术的发展，IT 设备集中管控将更加智能化和自动化。以下是一些未来趋势：

1. 物联网技术的应用：通过物联网技术，实现对 IT 设备的全面感知和实时监控，提高设备的管理效率和维护质量。

2. 智能技术的应用：通过智能技术，实现对 IT 设备的智能分析和预测，及时发现和解决问题，提高管理的智能化水平。

4. 主要功能简介

4.1. IT 设备集中运维

通过统一的 IT 运维监控管理平台，企业可从设备分类和业务信息系统视角出发，实现对服务器系统、网络、安全产品、操作系统、应用系统、储存设备、IT 环境等系统的状态和性能的实时监控。提供统一的用户界面，统一的管理手段，准确反映各类设备运行状态和性能。对于服务器系统及网络运行的异常表现进行预警，为优化 IT 系统性能和解决故障提供数据分析依据。

集中监控系统应支持无代理的监控方式，对各类应用服务器的配置数据、性能数据、告警数据进行采集。 同时集中监控管理系统能够通过监测工具自动定期监测服务器系统、网络系统、网络安全等设备的基本配置数据。

4.1.1. 设备状态集中监控

集中监控系统的监控视图实现对所有被监控对象告警的统一监控、集中展现。监控视图可以依据自身需求展示不同监控偏重的 IT 资源监控视图，如网络拓扑视图、资源状态视图、业务应用视图、安全视图、存储视图等。

4.1.2. 业务集中监控

系统提供灵活的业务定义方式，可以将网络、主机、应用、存储、虚拟化等 IT 资源作为相关业务的组成单元，从业务应用视角提供给客户对 IT 资源的监控方式。可以通过业务视图发现业务组件的故障点，从业务组件到对应的 IT 资源设备，实现完整 IT 资源监控和快速定位故障的效果。

业务信息监控系统应具有良好的开放性，提供便捷的录制工具，满足对不同应用系统的监控定制需求，便于用户对应用系统的监控部署。

可建立基于网络系统、服务器主机系统、网络安全硬件系统之上的企业综合业务监控管理系统:

能够监控各业务系统的整体运行效率；在监控整体效率的基础上，可将与业务系统相关联的 IT 资源分解， 可监控单个 IT 资源的执行效率，发现影响业务系统运行效率的系统和设备；

能够对业务系统涉及的 IT 资源进行灵活组合， 形成以业务视角的运行状态监控管理方式，从业务视角可查看各 IT 资源单元的运行状态。

4.1.3. 设备告警管理

通过对采集的 IT 资源数据，通过关联分析技术，提取有效的告警信息上报告警中心。

系统提供了灵活的告警设置，多样的告警推送方式。系统告警规则可实现快速设置，预置大量告警规则，提供基于设备类型指标参数的告警批量设置。告警的推送方式支持 syslog 外发、邮件、微信等。

系统提供灵活的告警查询方式，可通过告警检测指标进行统一查询，实现指标统一分析；也可通过设备 IP 查询该设备上所有的告警。

能够一键设备登陆跳转：基于平台智能处置引擎，可以按照流程一键登录业务系统进行处置操作，提高告警响应处置效率。

4.1.4. 自动运维巡检

系统可以按照 IT 运维的管理要求实现不同频度对不同设备运行状态的无人自动巡检，巡检的设备运行状态数据依据自主学习的业务基线以及业界规

范基准值进行分析检测；并将巡检异常以实时状态、越界统计、智能处置方式进行反应。

自动巡检对于不符合内置检测阈值的事件定义为告警事件，系统以告警事件的出现进行数据判断，提供完善的分析统计，包含等级、时间、指标、IP范围等基础信息。对于出现超过阈值的指标，系统通知相关运维人员。

统一下发式响应运维，例如版本过期时执行一键升级操作、安全设备策略统一下发、设备许可到期提醒等。

4.1.5. 运维编排

基于 SOAR 技术，结合工作流框架，将原本需要人员参与的事件处置流程转变为剧本。将事件处置过程中人、工具及能力、流程等参与元素和环节进行可视化组装编排，降低对人工参与的过度依赖。编排能力与平台进行深度结合，通过编排与运营两大体系协同作战增强运营合力。

平台独有的启发式联动响应能力，降低人员配置的复杂度，并在不依赖三方安全设备开放接口对接的前提下自动化执行响应剧本，进一步降低运营人员的工作负担，提升工作效率。

4.1.6. 设备日志收集

事件收集主要是对事件采集和格式化的过程。

- 聚铭睿合管控巡航平台能够支持以下事件源：

1. 防病毒、防火墙、入侵检测/防御系统等安全设备或系统；
2. 操作系统记录的重要安全相关的日志和事件告警，支持 Windows 2000/2003/NT/XP/Vista/7/2008/8，各种版本的 Linux/Unix 系统；
3. 各种类型的数据库日志，例如 Oracle、MySQL 等；
4. 防病毒系统、访问控制系统、用户集中管理和认证系统；
5. 各种应用系统的日志，如 Apache、Tomcat、IIS 等。

- 聚铭睿合管控巡航平台能够通过多种方式收集、分析各事件源发送的安全事件：

1. Syslog 方式：以 Syslog 方式接收安全事件；
2. SNMP trap：接收来自设备的 SNMP Trap 的事件；
3. 数据库方式：可以通过 JDBC 数据库接口获取事件源存放在各种数据库中的安全相关信息；支持的数据库类型包括 Oracle、Microsoft SQLServer、DB2、MySQL 和 Sysbase；
4. 网络 Socket 接口方式：可以通过 TCP/IP 网络，以 Socket 通信的方式获得安全事件；
5. 本地文件方式：可以通过读取事件源的日志文件，来获取其中与安全有关的信息；
6. 第三方代理或者应用程序：第三方的应用程序或者代理可以通过以上方式或者标准输出直接将安全事件转发给安全事件采集。

4.2. 资产管理

安全资产是聚铭睿合管控巡航平台的核心管理对象。与 ISO27001 的关于资产的定义略有不同，聚铭睿合管控巡航平台的资产是特指具有 IP 地址的 IT 类设备及其之上运行的、可管理的服务、应用。

4.2.1. 资产台账

一般而言，安全管理中的资产具备如下两类属性：

1. 基本属性：名称、编号、系统类型（产品类型、操作系统类型、版本等）、IP 地址（支持 IPv4 核 IPv6 格式）、响应人（出现安全问题应由何人处理）、登录凭证（获取配置、安全基线检查等使用）、上架信息等；

2. 安全属性：完整性、可用性、保密性、风险信息、开放端口、安全事件、漏洞、安全基线违规问题等。

聚铭睿合管控巡航平台的资产管理支持用户录入、导入或自动发现资产。

为了处理不同网络的资产同 IP 问题，聚铭睿合管控巡航平台还支持对于网络和 IP 地址段的管理。

为了用户便于集中、灵活地管理所辖范围内的资产，聚铭睿合管控巡航平台

支持用户自定义资产管理视图。

4.2.2. 拓扑管理

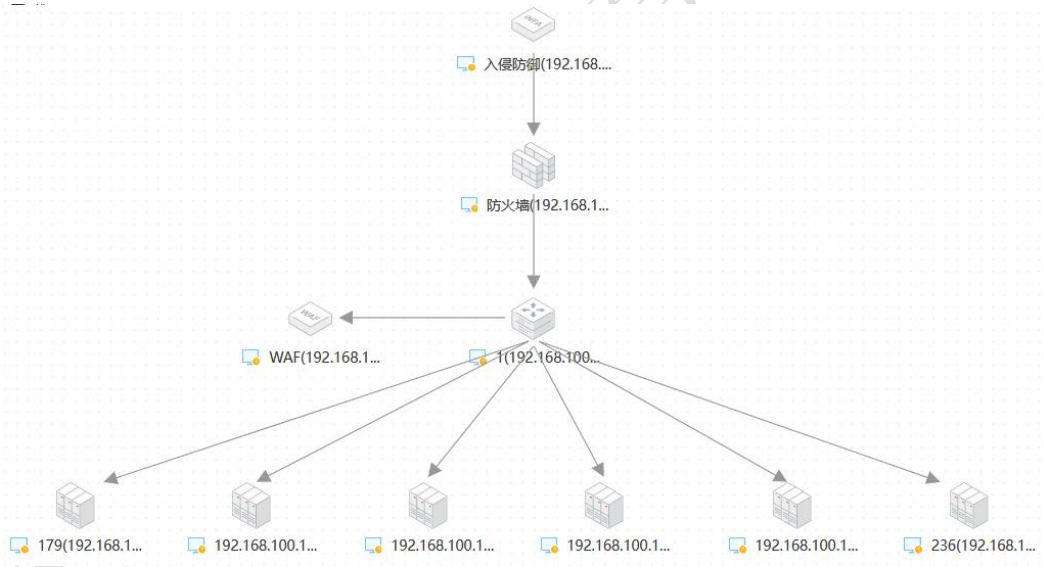
拓扑管理中提供了丰富的图元和工具，让用户可以编辑出多种多样的拓扑图。

➢ 工具包括：点选模式、框选模式、浏览模式、普通连线、折线、曲线、放大、缩小、1 比 1 展示、纵览展示、导出图片和打印预览。

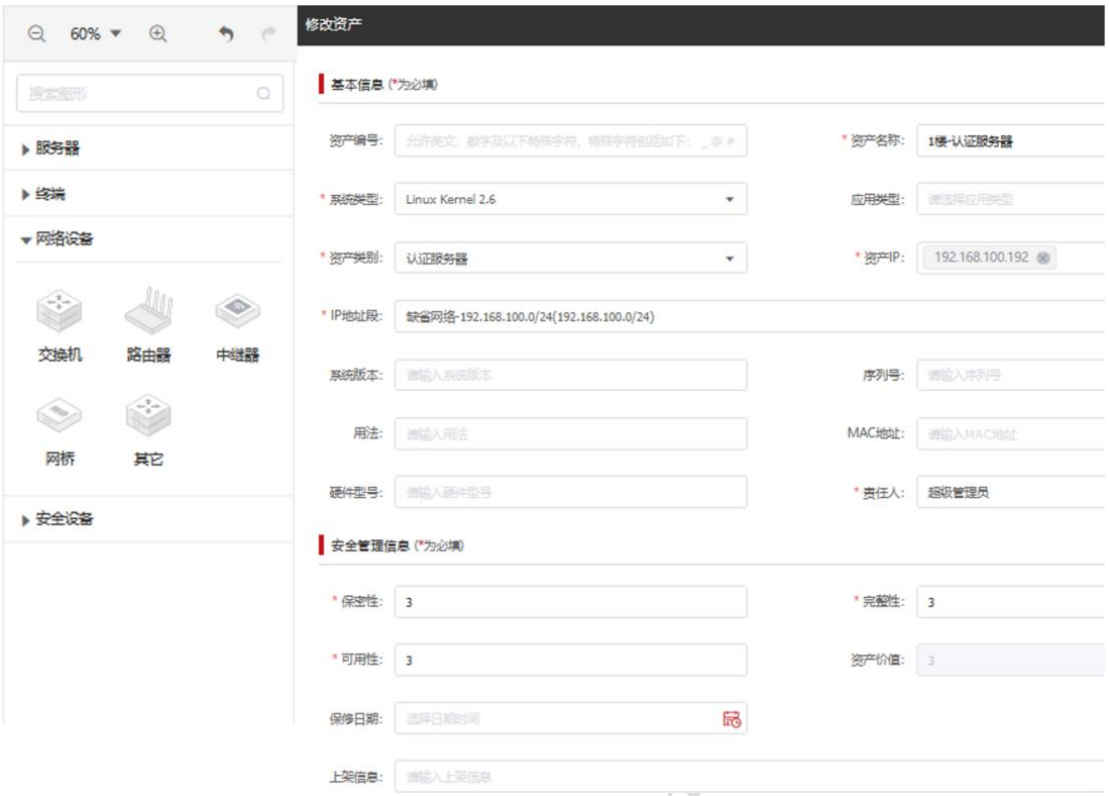
➢ 图元分为：背景类、设备类和其它类三大类，系统自带部分图元，同时支持用户自己上传。设备类图元可绑定资产，其它类中的人员可绑定系统中的用户信息，其它类中的视图图元可绑定系统中的视图信息。

➢ 端口信息配置：拓扑图中的连线中可配置连线两端的设备的端口信息。

➢ 子拓扑图配置：除设备类和背景类图元外，其它图元都可以创建下一级拓扑图。



拓扑管理中，用户可根据需要在左侧添加文字信息和微件信息，添加后效果如下图所示：



4.3. 运营仪表板

运营仪表板是聚铭睿合管控巡航平台风险的集中展示区域，也是系统展现给用户的第一个视觉界面；它支持以 TAB 页及微件（Widget）形式展现，用户也可对仪表的布局和内容进行定义和调整。

默认出厂，聚铭睿合管控巡航平台支持如下类型的仪表板：

1. 整体安全概况；
2. 资产概况；
3. 告警概况；
4. 安全事件概况；
5. 脆弱性概况；
6. 任务概况；
7. 工单概况。

4.4. 工单管理

工单是聚铭睿合管控巡航平台用于安全问题处理的一种形式，是安全运维支撑的流程体现。

当系统产生告警后，用户可以创建工单并分配给专人去处理。工单的状态包括待接受、处理中、已完成、求助、已关闭和作废等；而个人工单完成情况是供用户查看工单各种状态的分类信息。

4.5. 个人工作台

个人工作台是登录用户用于便捷操作的窗口。它固定的放置于页面的一个位置（通常是顶部），起到管理入口的作用。它主要包含了与登录用户相关的一些信息，但需对用户的权限进行过滤，其功能主要包括：

1. 对象快捷创建菜单，菜单中包含：资产、用户、任务（漏洞扫描、基线检查、资产发现）；
2. 个人待办事宜：工单、告警；
3. 通知功能：任务完成情况、工单情况；
4. 系统状态:每秒事件量（EPS）。

4.6. 报表管理

报表管理的作用为展示系统安全工作的结果。报表内容包含各种信息的统计情况，包括：告警报表、资产报表、安全事件报表、漏洞报表、安全基线报表、工单报表等。

用户可以定义相关条件以生成报表，它们均可以导出为 PDF、Word、HTML 等格式，如下图所示：

4.7. 知识库管理

知识库管理为系统运行和维护提供了知识来源以及安全问题的处理依据、方法或参考，目前支持如下几类：

1. 配置类：各种操作系统、网络设备、应用系统及数据库等接入 IT 运营管理平台日志的配置收集方法；

2. 安全事件/日志类：各种安全系统的报警以及操作系统、网络设备、服务器及数据库的日志信息；

3. 漏洞类：通过扫描器发现的在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷的描述及解决方案；

4. 安全基线类：各种操作系统、网络设备、防火墙、Web 中间件及数据库等可被威胁所利用而导致安全性问题的标准描述及解决方案；

5. 安全经验类：基于系统安全事件、漏洞、配置问题等信息综合生成的安全警示信息的描述、告警触发建议及解决方案等。

用户可以通过全文检索功能对系统提供的安全知识进行查询。

4.8. 系统管理

系统管理的主要功用在于管理支撑平台正常运行的各种基础功能和参数配置。主要功能有：用户管理、系统参数管理、内置对象管理、升级管理、许可证管理、日志管理、口令策略管理等。

5. 产品优势

- 提高设备利用率：集中管控可以实现对所有设备的统一监控和管理，通过合理调配和使用设备资源，提高设备利用率，减少资源浪费。
- 简化管理流程：集中管控可以实现各子系统的统一存储、显示和管理在同一平台上，从而简化设备管理流程，提高管理效率。
- 加强安全防范：集中管控可以实现对设备的全面监控和管理，及时发现并解决安全问题，保护企业的信息安全。
- 降低维护成本：集中管控可以减少 IT 设备维护的工作量和成本，因为所有的设备都集中在同一平台上进行管理，维护起来更加方便快捷。
- 适应业务需求：集中管控可以根据不同的业务需求，灵活调整设备资源配置，更好地满足企业的业务需求。