功能概述

统信服务器运维监管平台（又名“统信有幄”，英文名为“UnionTechMaintenance and Operation Platform”，缩写为“UMOP”）是一款专为服务器操作系统打造的企业级可视化自动运维软件。平台基于模块化、插件化设计理统信服务器运维监管平台，集“监、管、控、安全”为一体，适用于传统数据中心及云数据中心场景，切实减轻企业快速数字化转型进程中与日俱增的运维压力，为企业提供简单、易用、安全、高效的全方位一体化解决方案。



图1.1 产品架构图

1. 主机管理

基础多款0S版本主机的批量导入导出、基于Web远程运维等。

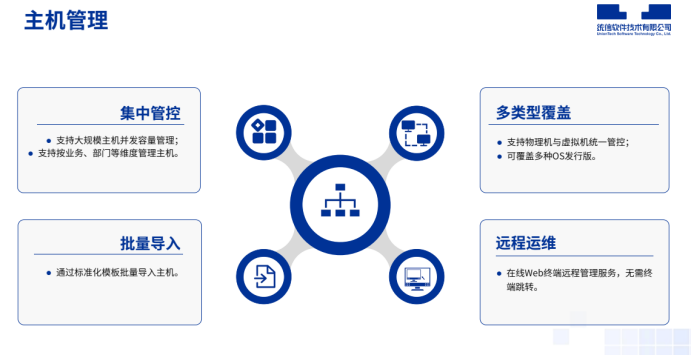


图2.1 主机管理

2. 系统监控

实时监控资源使用情况、异常事件与用户行为等。



图2.2 系统监控

3. 配置下发

批量配置文件下发、定期密码修改。

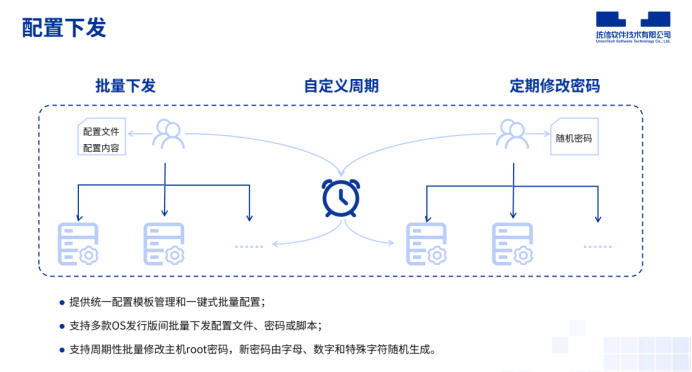


图2.3 配置下发

4. 安全管控

CVE漏洞自动扫描与一键修复、防火墙规则自生成、用户权限管控等。



图2.4 安全管控

5. 诊断分析

内核级诊断能力，可从调度、存储、网络及内存多维度深入分析。



图2.5 诊断分析

6. 告警服务

提供系统资源、主机心跳类报警，通过网页、企微和钉钉方式推送报警。

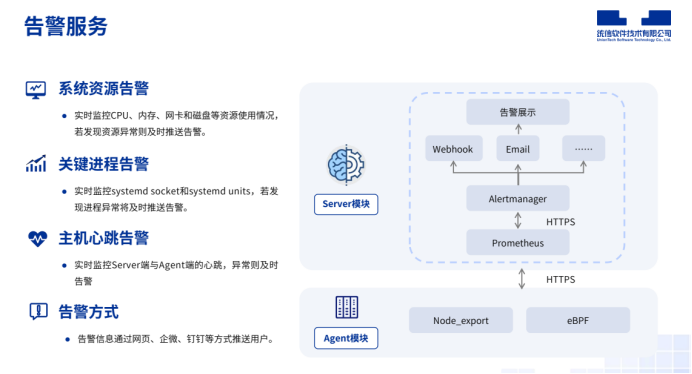


图2.6 告警服务

功能介绍

1. 产品功能

1.1. 主机管理

统信有幄支持集中管控、多类型覆盖、批量导入和远程运维功能，解决多种服务器操作系统发行版的大规模集中管理的难题。

(1) 集中管控

统信有幄支持大规模主机并发容量管理，满足中大型企业服务器操作系统的运维监管需求。支持集群管理，可按照业务、部门、地域或产品维度来分类管理被纳管主机。

(2) 批量导入

统信有幄支持通过 Excel 模板批量导入主机功能，通过创建集群并完成预设模板编辑（录入主机名称、IP 地址、端口、登录用户等主机信息）即可完成大规模主机信息的一键导入。

(3) 多类型覆盖统信有幄支持同时纳管物理主机和虚拟主机，适用于传统数据中心和云场景。在网络连通范围内，只要部署了统信有幄可兼容的操作系统（如CentOS等）的主机，都可被统信有幄统一纳管。

(4) 远程运维

统信有幄提供在线终端功能，通过浏览器实现对远程服务器的免密登录与管理，并可将指定程序的输入输出重定向到网页上。

1.2.  系统监控

监控是运维过程中最基础的一环。为提升服务器操作系统运维质量，保障业务系统的持续稳定运行，统信有幄提供系统监控功能，可从资源、事件、安全及用户等维度深层次采集系统各项关键指标数据，实时跟踪集群中各主机运行状态，及时发现和预警系统问题。

(1) 资源监控

统信有幄可实时展示 CPU 算力、内存、磁盘以及网络带宽、网络延时等关键指标的时序曲线，使运维人员能直观地查看各项指标运行情况，并在操作系统出现异常时及时发现和定位问题。

(2) 事件监控

统信有幄支持对 Kernel Panic（内核崩溃）等主机宕机事件的监控。当内核崩溃时，Kdump 内核崩溃转储机制将启动预先配置好的附加内核，并记录发生故障的生产内核状态，生成 vmcore 文件。当平台监测到vmcore 文件生成时，会在 Web 控制台实时展示 vmcore 文件信息（如宕机事件发生时间、主机内核版本等），同时以告警方式通知相关运维人员。

(3) 安全监控

统信有幄基于 Errata 机制实现 CVE 漏洞监控能力，依托统信应急响应中心（USRC）漏洞库对被纳管主机进行周期性漏洞扫描。默认情况下，平台每天凌晨会进行一次 CVE 漏洞扫描，扫描完成后立即出具修复建议（如：漏洞信息、漏洞严重等级、漏洞发布事件、漏洞涉及到的主机等）。统 信 应 急 响 应 中 心 （ USRC ） 地 址详见如下链接：https://src.uniontech.com/index.php?m=&c=index&a=index

(4) 用户监控

统信有幄支持用户行为审计与监视，提供用户 IP、请求方法以及行为类型、操作结果等信息的实时记录功能。当出现问题没有日志记录或依靠现有日志无法定位问题时，可通过分析用户行为进行事后追溯，以及时发现非法操作，缩短故障排查时间。

1.3. 配置下发

运维人员在管理大规模（百台及以上）服务器操作系统时，经常面临批量配置被纳管主机的情况，若采用人工方式逐台配置，不仅耗时、耗力，还可能因误操作造成系统瘫痪、业务中断等无法估量的后果。针对此问题，统信有幄提供统一配置模板管理和一键式批量配置功能，可对集群中指定主机统一下发配置文件、密码和脚本，而无需考虑集群中不同操作系统发行版之间的接口和配置差异。对于安全性要求较高的客户，统信有幄提供周期性批量修改密码功能，可在指定时间自动修改集群内指定主机 root 密码，新密码必须是字母、数字和特殊字符的随机组合。

1.4. 安全管控

漏洞是操作系统或应用软件本身的一种缺陷，一旦被攻击者发现就很容易被攻击者利用，从而在系统未授权状态下访问或破坏操作系统。为尽早发现漏洞，及时消除安全隐患，统信有幄提供安全管控功能，通过主动漏洞防护、多漏洞统一管理、防火墙规则自生成以及主机口令增强和用户权限管控等手段提升集群内统信主机安全性。

(1) 主动漏洞防护：满足内外网场景，支持人工扫描及定期自动漏洞扫描，支持漏洞批量修复；

(2) 多漏洞库统一管理：可对接统信及第三方漏洞库，实现多来源漏洞数据的统一关联；

(3) 防火墙规则自生成：支持防火墙规则根据业务报文信息自动生成；

(4) 主机口令增强：支持定期批量修改密码；

(5) 权限管控：支持主机权限管控，通过自定义角色方式保障集群最小赋权。除此之外，统信有幄采用 B/S 架构设计，由 Agent 端和Sever 端两部分构成，为提升自身安全性，Agent 端将采集的数据通过 HTTPS 和Basic Auth认证加密后传送至 Server 端处理，Server 端将处理后的数据通过AES 加密存储至数据库，确保数据全流程安全可靠。

1.5. 诊断分析

统信有幄为降低操作系统运维难度、缩短排障时间，基于业内领先的eBPF技术打造系统级自动诊断分析方案。该方案可全链路分析和诊断系统关键指标并快速定位问题，将系统问题诊断标准化、自动化，实现对服务器操作系统的日常运维场景全覆盖，如健康诊断、调度异常、I/O 延时以及网络延时、内存异常等。

(1) 健康诊断

统信有幄提供一键健康诊断功能，可深入剖析系统整体运行状态，预判系统健康度，提前发现和防范系统问题。健康诊断的检查内容主要包括配置异常检查、OS 指标检查和异常指标诊断、宕机自动分析、OS 日志异常分析、硬件问题识别等。

(2) 调度异常诊断

统信有幄提供系统调度诊断功能，可针对影响系统调度的关键信息提供诊断分析，如硬中断、软中断、进程 R/D 状态、进度调度等。通过遍历所有进程调度、中断信息整合计算出系统调度情况并绘制调度火焰图。

(3) I/O 延时诊断

统信有幄提供磁盘 I/O 读写延时诊断功能，当操作系统出现磁盘写操作慢（延时）异常时，运维人员只需要在 Web 页面指定写延时的磁盘和延时超时时间就可交由工具自动跟踪诊断，无需运维人员采取加入断点、打印日志等方式手动跟踪，提高异常诊断效率。

(4) 网络延时诊断

统信有幄提供网络报文时延与抖动诊断功能，可基于ICMP 协议探测网络时延并确定问题边界。诊断开始后，统信有幄将从 Server 端向Agent 端发送PingTrace 时延探测报文，并实时展示数据链路中每阶段时延情况，快速诊断出问题边界。

(5) 内存异常诊断

内存泄露、内存碎片以及内存占用排序这类系统内存异常类问题对运维人员的专业技能要求很高，通常需资深运维人员才能解决。统信有幄集成内存异常一键诊断工具，将原来依赖经验丰富运维人员的工作转化为标准化工具，实现复杂问题的自动化诊断与分析，比如通过展示内存消耗最多Top 10 进程和缓存文件Top 10 信息，方便运维人员定位内存泄露情况，以及通过对比预设的度量指标确认内存碎片的严重程度。

1.6. 告警管理

统信有幄提供告警管理功能，可自定义告警规则和配置通知策略。当集群中的主机触发告警规则条件时，平台将根据预先配置的通知策略向运维人员发送告警信息，使运维人员及时发现异常，尽早处理问题。

当前，统信有幄已支持企业微信、钉钉等 Webhook 类告警，可对接日常即时聊天工具，当发现异常情况时将自动向运维人员推送告警信息。

2. 产品特性

2.1. 一站式

统信有幄对运维入口、配置管理、权限管控和监控视图等功能的操作进行了整合，可在同一个平台上完成主机管理、系统监控、异常诊断、日志审计、安全管控等复杂运维管理，通过一站式系统运维管理能力，解决软件重复建设与运维工具碎片化问题。

(1) 统一运维入口

针对监控、配置与安全管理等模块入口分离现状，统信有幄通过统一的运维入口实现多模块数据共享复用，提供更强大的运维支撑能力。

(2) 统一配置管理

统信有幄可对分散于集群中的各类主机（物理主机和虚拟主机）统一下发配置文件、密码和脚本，屏蔽了主机之间环境差异（账户、主机名、文件路径等各不相同）和操作系统版本差异，实现配置的集中管理，把复杂问题简单化。

(3) 统一权限管控

所有功能模块共用一套权限管控机制，解决多账户权限管理混乱问题，实现统一的权限访问管控，确保用户身份安全合法，更合规。

(4) 统一监控视图

使用统一监控视图展示多样化监控数据，帮助运维人员多维度观测所管理主机状态，以快速发现和定位问题，提升运维决策效率。

2.2. 模块化

统信有幄采用松耦合方式构建，将各功能模块进行细粒度拆解，实现不同模块以不同应用程序启动，如主机管理、监控、诊断、安全等，可依据不同业务场景实现不同模块组合的按需部署，给用户更多选择。

与此同时，统信有幄提供与操作系统相关的个性化定制化服务，如定制系统安全加固方案、定制平台告警方式等。

此外，统信有幄提供开放式 API，可根据用户场景实现二次开发定制。其全新的动态插桩式技术使得统信有幄功能模块可以方便的嵌入用户已有运维监管平台，提升用户统一运维能力。

2.3. 易用性

统信有幄基于开源框架对安装部署、操作管理等功能进行大量优化，并通过可视化运维方式，提升运维使用体验，降低运维难度。

(1) 易部署

统信有幄支持一键快速安装，有效提升部署效率；并且部署时安装包可自适应 CPU 平台，为不同架构下的安装提供一致的运行体验。

(2) 易操作

统信有幄以折线图、趋势图等图表形式将大量复杂的系统和设备参数数据予以友好展示，使数据更贴合客户场景，清晰易解读。所有操作均可通过Web可视化方式执行，将复杂配置和管理流程以一目了然的形式呈现。针对内存泄露、内存碎片这类只有资深运维人员才能定位的疑难问题，提供自动诊断分析工具，使普通用户也能轻松定位问题，降低运维门槛。

2.4. 自动化

统信有幄将自动化理念融入操作系统运维管理中，实现运维自动化，通过系统自动监控、异常自动发现以及问题自动诊断，可有效减少重复性工作，降低人工误操作概率，提升运维效率。

(1) 系统自动监控

通过多维度监控体系加强系统异常感知能力，预防和减少故障损失。

(2) 异常自动发现

通过异常事件告警、漏洞自动扫描机制等，更早发现问题。

(3) 问题自动诊断

如系统健康度、网络延时等复杂问题的自动诊断与定位，可缩短问题解决时间，有效提升工作效率。

2.5. 强安全

统信有幄继承了统信服务器操作系统的安全特性，高度重视系统以及各类数据的安全性，将多种安全策略和安全机制予以有机组合，围绕用户所管理主机提供全方位的漏洞管理、日志审计和身份认证能力，满足用户各类安全要求。

(1) 漏洞管理

统信有幄主动漏洞防护方案可实时同步最新漏洞信息，自动扫描与评估漏洞情况，全程跟踪漏洞修补进度，使集群内系统及数据的安全得以有效保障，提升企业漏洞治理能力。

(2) 日志审计

全程记录用户登录、操作和访问信息，实时监管运维过程，满足事后溯源和行为审计需求，提升运维合规性。

(3) 身份认证

针对用户权限进行分角色、分范围、分类别的精细化设计，实现用户账号统一集中管理，让合法人员管理权限内的主机，预防非法操作发生，保障系统的安全合规性。

2.6. 泛兼容

统信有幄支持主流国内外处理器架构，提供对主流服务器操作系统发行版本的统一纳管，满足跨浏览器兼容性，为用户监管大规模服务器操作系统提供更多选择。

(1) 多架构兼容

统信有幄支持国内外主流处理器架构（AMD64 和ARM64）主流服务器硬件的良好适配。

(2) 多发行版兼容

支持统信服务器操作系统 V20、CentOS 7/8 等发行版。

(3) 跨浏览器兼容

统信有幄通过对 Chrome 与 Firefox 等主流浏览器的兼容，实现各平台运行体验的一致性，给拥有不同浏览器偏好的用户更多选择。

(4) 第三方漏洞库对接

统信有幄支持引入第三方漏洞数据源，支持 JSON 离线文件形式导入，或以在线 URL 访问方式添加第三方漏洞数据源，实现多来源漏洞数据的统一关联，满足用户对已有漏洞库的再利用需求。

©统信软件技术有限公司。访问者可将本网站提供的内容或服务用于个人学习、研究或欣赏，以及其他非商业性或非盈利性用途，但同时应遵守著作权法及其他相关法律的规定，不得侵犯本网站及相关权利人的合法权利。除此以外，将本网站任何内容或服务进行转载，须备注：**该文档出自【faq.uniontech.com】统信软件知识分享平台**。否则统信软件将追究相关版权责任。