

The background of the slide is a complex, abstract graphic. It features a dark blue and black base with glowing blue and green lines that resemble a circuit board or a network diagram. There are also some faint, stylized icons, such as a padlock, scattered throughout the design. The overall aesthetic is high-tech and digital.

华康安全运维
管理系统
HC-OMS

北京力控华康科技有限公司

www.sunwayland.com



目录

产品概述 02

产品架构 04

产品特点 05

典型应用 08

产品概述

随着IT建设的不断深入和完善,计算机软硬件系统的运行维护已经成为了各行各业各单位领导和信息服务部门普遍关注和不堪重负的问题。由于这是随着计算机信息技术的深入应用而产生的,因此如何进行有效的IT运维管理,这方面的知识积累和应用技术还刚刚起步。对这一领域的研究和探索,将具有广阔的发展前景和巨大的现实意义。

大中型企业和机构纷纷建立起庞大而复杂的IT系统,IT系统的运营、维护和管理的风险不断加大。运维管理安全风险是指**运维用户在运维操作中引入的风险,包括变更设计不完善、误操作、越权操作、恶意操作及代维等因素**。由于运维管理一般是采用特权用户进行操作,所以其操作风险非常大。目前大多数用户采用分权双人、多种管理制度等方式来规避或降低安全风险,但实际运行中由于制度未落实等问题,无法做到全面的控制,运维安全仍然存在很大的风险。



“ 运维用户在运维操作中引入的风险,包括变更设计不完善、误操作、越权操作、恶意操作及代维等因素。 ”

1. 运维操作复杂度高

随着企业系统、网络规模的扩大,设备的增多,设备管理人员也相应的增多;由于运维用户角色及设备功能的不同,会存在同一个运维用户同时管理多台设备,也会存在同一台设备被多个运维用户共同管理;由于多个运维用户需要登录同一台设备,因此该设备的账号密码是共用的,无法对账号密码进行有效管理;同时这样的交叉管理会造成运维用户的违规操作和越权访问,并且无法实现有效的监管。

2. 运维操作不透明

由于IT运维操作的复杂度,致使我们无法知道运维用户在过去和现在都对设备进行了哪些操作,这些操作是否会对设备及业务造成影响;而一旦出现问题,企业IT部门也无法追溯到是谁在什么时候以及做了哪些操作导致出现问题;其实企业都有一定的制度来控制设备账号以及运维用户权限,但由于没有技术保障,很难被完全地执行。

3. 误操作给企业带来严重损失

运维操作的复杂难免会造成运维用户的误操作,这些误操作一旦涉及到敏感的操作命令,就有可能造成网络中断从而影响企业业务运行,也有可能导企业核心数据被修改或删除。

4. 运维外包给企业带来管理风险

IT运维外包带来了一定效率的提高,但企业无法直接有效地管理外包人员,无法对外包人员的操作行为做到有效的控制和监管,甚至无法确保外包人员不会破坏或窃取企业设备、数据。

5. 法律法规的要求

IT系统审计是控制内部风险的一个重要手段,但IT系统构成复杂,操作人员众多,如何有效地对其进行审计,是长期困扰各组织的信息科技和风险稽核部门的一个重大问题。而由于信息系统的脆弱性、技术的复杂性、操作的人为因素,企业目前无法实现对各类系统及网络设备的运维操作进行实时监控和审计;同时虽然企业能定期修改设备的密码,但由于设备的交叉管理,无法确保设备密码的安全性,也就无法有效地保障企业的信息安全。

6. 人员流动性给企业带来未知风险

企业IT人员的流动性会给企业IT运维的延续性带来一定影响,每次IT员工的离开,都需要立即更改该员工所管理的设备的账户密码,否则会给企业信息安全带来风险,而由于设备的交叉管理,会导致变更操作非常麻烦。

国际著名咨询调查机构Gartner集团的调查发现,在经常出现的运维问题中,源自技术或产品本身方面的问题其实只占20%,而操作流程失误问题占40%,人员的误操作问题占40%。面对这种情形,企业需要一套完善的运维管理解决方案。

1. 设备集中统一管理

运维用户通过一个统一的平台就能登录所有的目标设备,包括Unix、Linux、Windows服务器以及各类网络设备,并且运维用户不需要知道目标设备的账户密码;同时目标设备的密码可以依据企业策略定期自动修改。

2. 根据策略实现对操作的控制管理

根据企业的策略,控制哪些运维用户、可以通过什么样的权限、在什么时间、访问哪些目标设备,从而能够有效地控制运维用户的操作权限,降低运维操作的复杂度。

3. 实时的操作告警及审计机制

运维操作的复杂难免会造成运维用户的误操作,企业需要避免由此带来的风险,同时需要拥有问题追溯机制。这就要求能对运维用户的所有操作进行实时的控制、告警及监控,避免由于一些敏感的操作导致网络中断或企业信息泄露,同时能记录所有操作并能随时根据审计的需要查询任何时候任何人员所做的任何操作,并有详尽的报表。

4. 符合法律法规

针对安然、世通等财务欺诈事件,2002年出台的《公众公司会计改革和投资者保护法》(Sarbanes - Oxley Act)对组织治理、财务会计、监管审计制定了新的准则,并要求组织治理核心如董事会、高层管理、内外部审计在评估和报告组织内部控制的有效性和充分性中发挥关键作用。与此同时,国内相关职能部门亦在内部控制与风险管理方面制定了相应的指引和规范。

由于信息系统的脆弱性、技术的复杂性、操作的人为因素,在设计以预防、减少或消除潜在风险为目标的安全架构时,引入运维管理与操作监控机制来预防、发现错误或违规事件,对IT风险进行事前防范、事中控制、事后审计的组合管理是十分必要的。

5. 易部署、高可用性

除了以上管理和审计需求,首先要确保产品能够快速、方便的部署,且不影响用户的原有操作习惯;其次要保证设备自身的安全性、稳定性及高可用性,避免单点故障。

产品简介

华康安全运维管理系统(简称:堡垒机)可对主机、服务器、网络设备、安全设备等的管理维护进行安全、有效、直观的操作审计,对策略配置、系统维护、内部访问等进行详细的记录,提供细粒度的审计,并支持操作过程的全程回放。

华康安全运维管理系统弥补了传统审计系统的不足,将运维审计由事件审计提升为内容审计,并将身份认证、授权、管理、审计有机结合,保证只有合法用户才能使用其拥有运维权限的关键资源。

华康安全运维管理系统为组织在IT操作风险控制、内控安全和合规性等方面提供了完善、有效的审计手段。



华康安全运维管理系统的部署可将企业的IT办公虚拟化。员工办公之前统一登录到华康安全运维管理系统,再由华康安全运维管理系统自动登录到各类办公服务器。员工所有的办公其实都是远程登录到服务器上,所有的操作和资料都存储在服务器,员工的办公电脑就好比一台显示器。完全杜绝文档拷贝与传递,防止本地打印,杜绝机密文件的传输与泄漏。同时也能很好地对企业的资料进行统一管理与存储。

华康安全运维管理系统支持Telnet、FTP、SSH、SFTP、RDP (Windows Terminal)、Xwindows、VNC、HTTP、HTTPS等多种通信协议,支持IBM AIX、Digital UNIX、HP UNIX、SUN Solaris、SCO UNIX、LINUX、WINDOWS等多种操作系统。可广泛应用于金融、政府、电信、证券、邮政、税务、海关、交通等安全需求较高的行业。

产品架构

运维事件事前防范

1.完整的身份管理和认证

为了确保合法用户才能访问其拥有权限的后台资源,解决IT系统中普遍存在的交叉运维而无法定位到具体人的问题。满足“谁能做”的授权需求和“谁做的”审计系统要求,系统提供一套完整的身份管理和认证功能。

1) 支持用户分组管理。

2) 支持运维用户静态密码、USBKey、指纹、OTP认证、口令+短信、口令+ USBKey、Radius、LADP、AD域、POP3、TACACS+认证方式。

3) 支持密码强度、密码有效期、密码尝试锁死等安全管理功能。

4) 支持用户信息导入导出,方便批量处理。

2.灵活、细粒度的授权

系统提供基于运维用户、运维协议、目标主机、运维时间段、运维会话时长、运维客户端IP等组合的授权功能,实现细粒度授权功能,满足用户实际授权的需求。

1) 提供基于运维用户到资源的授权。

2) 提供基于运维用户组到资源的授权。

3) 提供基于运维用户到资源组的授权。

4) 提供基于运维用户组到资源组的授权。

5) 运维用户只能看见和执行已授权的应用软件。

6) 支持管理员角色及功能模块细分。

7) 提供管理员对不同运维用户的分管机制。

3.后台资源自动登录

后台资源自动登录功能是运维用户通过华康安全运维管理系统认证和授权后,华康安全运维管理系统根据配置策略实现后台资源的自动登录,运维用户无需知道后台资源的账户密码。此功能提供了运维用户到后台资源账户的可控对应,同时实现了对后台资源账户口令的统一保护。

针对不同主机、网络和安全设备的特性,华康安全运维管理系统提供对账户口令托管和只托不管两种方式实现运维用户自动登录后台资源。

1) 托管方式实现自动登录后台资源

华康安全运维管理系统自动获取后台资源账户信息。

根据口令安全策略,华康安全运维管理系统定期自动修改后台资源账户口令。

根据管理员配置,实现运维用户与后台资源账户对应,限制账户的越权使用。

运维用户通过华康安全运维管理系统认证和授权后,华康安全运维管理系统根据分配的账户自动登录后台资源。

2) 只托不管方式实现自动登录后台资源

管理员将后台资源账户及口令配置到华康安全运维管理系统中。

根据管理员配置,实现运维用户与后台资源账户对应,限制账户的越权使用。

运维用户通过华康安全运维管理系统认证和授权后,华康安全运维管理系统根据分配的账户自动登录后台资源。

运维事件中控制

1. 实时监控

监控正在运维的会话,信息包括运维用户、运维客户端IP地址、资源IP地址、协议、开始时间等。

监控哪些后台资源当前正在被访问。

提供在线运维操作的实时监控功能。

对正在运维的资源,根据管理需要可立即中断运维会话。

2. 违规操作实时告警与阻断

针对运维过程中可能存在的潜在操作风险,华康安全运维管理系统根据用户配置的安全策略对运维过程中的违规操作进行检测,对违规操作提供实时告警和阻断,从而达到降低操作风险及提高安全管理与控制的能力。

对于字符型协议,支持配置任何命令告警;对于文件协议,支持十多种常见的关键命令告警;对于数据库协议,支持二十多种常见SQL类型的告警。

告警动作支持会话阻断、审计平台告警、邮件告警、短信告警等。

产品特点

全面的运维审计

系统采用协议分析、基于数据包还原虚拟化技术,实现操作界面模拟,将所有的操作转换为图形化界面予以展现,实现100%审计信息不丢失。

针对运维操作图形化审计功能的展现外,同时还能对字符进行分析,包括命令行操作的命令以及回显信息和键盘、

运维事件事后审计

1. 完整记录网络会话过程

系统提供运维协议Telnet、FTP、SSH、SFTP、RDP (Windows Terminal)、XWindows、VNC、HTTP、HTTPS、MYSQL、DB2、SQL SERVER、SYBASE、ORACLE、INFORMIX等网络会话的完整会话记录,完全满足内容审计中信息百分百不丢失的要求。

会话信息包括运维用户、运维地址、后台资源地址、资源名、协议、起始时间、终止时间、流量大小信息。

会话信息包括运维过程中所有进出后台资源的数据。

2. 详尽的会话审计与回放

运维操作审计以会话为单位,提供当日和条件查询定位。条件查询支持按运维用户、运维地址、后台资源地址、协议、起始时间、结束时间和操作内容中关键字等组合方式。

针对命令交互方式的协议,提供逐条命令及相关操作结果的显示。

提供图像形式的回放,真实、直观、可视地重现当时的操作过程。

回放提供快放、慢放、拖拉等方式,方便快速定位和查看。

针对命令交互方式的协议,提供按命令和时间进行定点回放。

针对RDP、Xwindows、VNC协议,提供按时间和键盘输入进行定点回放。

针对HTTP、HTTPS、MYSQL、DB2、SQL SERVER、ORACLE、SYBASE、DB2、INFORMIX协议,提供按时间、URL或SQL进行定点回放。

3. 完备的审计报表功能

华康安全运维管理系统提供多种维度的报表,如基于时间、用户、资源、协议、用户组、资源组和告警统计的报表。支持在线实时定时自动报表。

鼠标的操作信息。

系统支持的审计协议以及工具包括:

终端命令操作:Telnet、SSH

Windows图形:RDP、VNC等

Unix/Linux图形:Xwindows

文件上传和下载:FTP、SFTP、SCP

基于BS的管理操作:HTTP、HTTPS

数据库协议:ORACLE、SQL SERVER、MYSQL、SYBASE
(工具用户自行发布)、DB2、INFORMIX (工具用户自行发布)

应用发布协议:用户使用应用发布发布的自定义协议。

友好的协同运维支持

系统针对常见的运维协议SSH、TELNET、RDP、VNC提供了协同运维功能。当运维人员运维时遇到困难或者需要双人一起运维的时候可以使用该功能,两个运维人员一起运维同一个资源,大家同时都具有读写权限,可以协同完成对资源的运维。

强大的应用发布支持

通过专业的应用发布系统配合华康安全运维管理系统发布维护工具,如PCAnywhere、dame ware、常用数据库工具、常用运维工具等,能够完美支持用户按照实际需求对华康安全运维管理系统进行扩展。

方便的批量管理

系统提供批量脚本和批量命令实时及定时执行的功能,减少运维人员反复地进行重复性工作,提高工作效率,降低运维成本。如图:

安全运维管理系统
Security Operations Management System

opuser

首页 | 批量管理

任务管理 脚本管理 命令管理

任务名称:

序号	任务名称	任务类型	脚本/命令名称	状态	描述	操作
1	test	命令	test			<input type="button" value="删除"/> <input type="button" value="刷新"/>

显示 1 - 1 条, 共计 1 条

系统持续运行: 6天8小时31分秒 安全运维管理系统 2019年10月22日 18:24:04

全面IPV4/IPV6支持

系统提供的所有功能都支持IPV4、IPV6双协议栈。

丰富的运维方式

系统提供客户端方式运维和web方式运维。

对于图形类协议及HTTP、HTTPS、ORACLE、SQL SERVER、MYSQL、DB2等协议,系统还额外提供mstsc remoteapp 和web remoteapp方式运维。

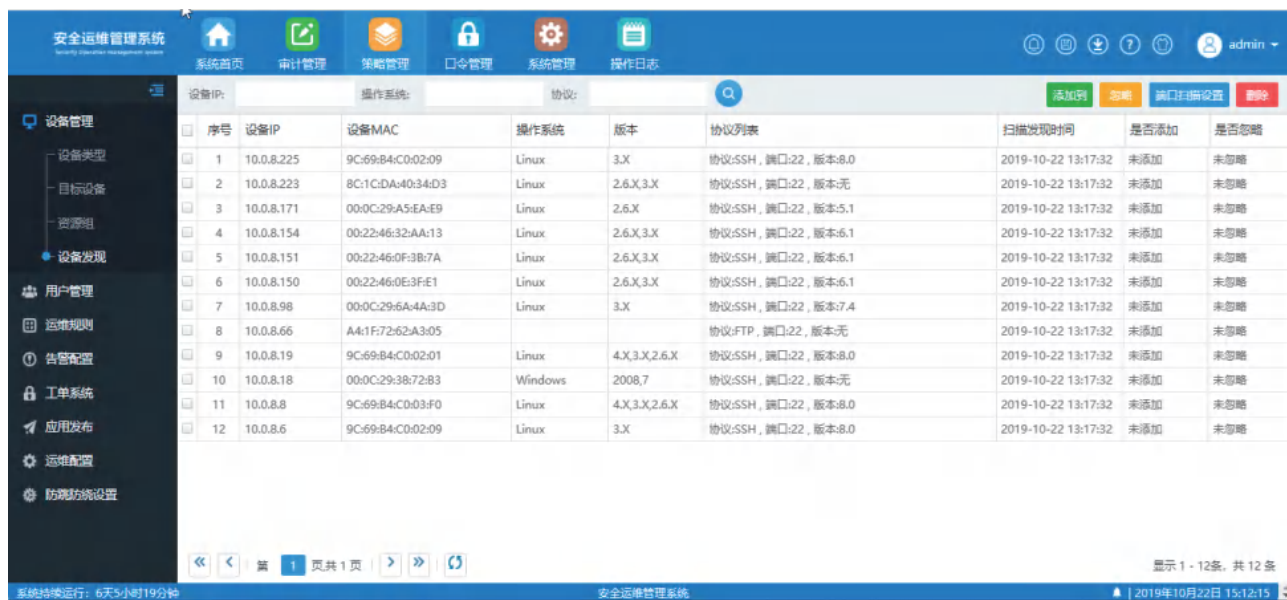
对于HTTP、HTTPS协议,系统提供内置3种浏览器方式的运维,分别为Chrome、Firefox和IE11。

易部署高可用

系统提供单臂、中间机2种模式接入到企业内部网络中,无需改变网络拓扑,安装调试过程简单。同时系统支持双机热备功能,提高容错率,避免单点故障,保障用户的正常业务开展。

智能的设备发现功能

系统提供了一种智能发现网络中的设备及协议功能,并支持一键式添加到策略,简化运维管理员繁琐的操作,同时减少遗漏,提高运维的效率。如图:



序号	设备IP	设备MAC	操作系统	版本	协议列表	扫描发现时间	是否添加	是否忽略
1	10.0.8.225	9C:69:84:C0:02:09	Linux	3.X	协议:SSH, 端口:22, 版本:8.0	2019-10-22 13:17:32	未添加	未忽略
2	10.0.8.223	8C:1C:DA:40:34:D3	Linux	2.6.X,3.X	协议:SSH, 端口:22, 版本:无	2019-10-22 13:17:32	未添加	未忽略
3	10.0.8.171	00:0C:29:A5:EA:E9	Linux	2.6.X	协议:SSH, 端口:22, 版本:5.1	2019-10-22 13:17:32	未添加	未忽略
4	10.0.8.154	00:22:46:32:AA:13	Linux	2.6.X,3.X	协议:SSH, 端口:22, 版本:6.1	2019-10-22 13:17:32	未添加	未忽略
5	10.0.8.151	00:22:46:0F:3B:7A	Linux	2.6.X,3.X	协议:SSH, 端口:22, 版本:6.1	2019-10-22 13:17:32	未添加	未忽略
6	10.0.8.150	00:22:46:0E:3F:E1	Linux	2.6.X,3.X	协议:SSH, 端口:22, 版本:6.1	2019-10-22 13:17:32	未添加	未忽略
7	10.0.8.98	00:0C:29:6A:4A:3D	Linux	3.X	协议:SSH, 端口:22, 版本:7.4	2019-10-22 13:17:32	未添加	未忽略
8	10.0.8.66	A4:1F:72:62:A3:05			协议:FTP, 端口:22, 版本:无	2019-10-22 13:17:32	未添加	未忽略
9	10.0.8.19	9C:69:84:C0:02:01	Linux	4.X,3.X,2.6.X	协议:SSH, 端口:22, 版本:8.0	2019-10-22 13:17:32	未添加	未忽略
10	10.0.8.18	00:0C:29:38:72:83	Windows	2008,7	协议:SSH, 端口:22, 版本:无	2019-10-22 13:17:32	未添加	未忽略
11	10.0.8.8	9C:69:84:C0:03:F0	Linux	4.X,3.X,2.6.X	协议:SSH, 端口:22, 版本:8.0	2019-10-22 13:17:32	未添加	未忽略
12	10.0.8.6	9C:69:84:C0:02:09	Linux	3.X	协议:SSH, 端口:22, 版本:8.0	2019-10-22 13:17:32	未添加	未忽略

更严格的审计管理

系统提供默认的三权分立的管理模式,包括系统管理员、运维管理员和审计员三种管理员角色,同时支持灵活定制管理员角色,进一步细化管理员权限,从技术上保证系统管理安全。

系统提供不同管理员对运维用户的分管机制,方便多管理员分权管理。

系统将认证、授权、管理和审计有机地集成为一体,有效地实现了事前预防、事中控制和事后审计。

丰富实时的报表系统

报表系统实时生成,且支持多种业务维度。

系统提供多种报表格式,包括PDF、Word、Excel、HTML、PPT。

系统提供直接html打印。

高效的处理能力

系统具有业界最强的协议转发处理能力,摒弃业界常用的协议转发“黑盒子”,能够对Telnet、FTP、SSH、SFTP、RDP (Windows Terminal)、Xwindows、VNC、HTTP、HTTPS等协议进行完整的透明转发,特别是对图形化操作协议的转发性能远远优于其它同类型产品。

完善的系统安全设计

精简的内核和优化的TCP/IP协议栈。

基于HTTPS/SSL的自身安全管理与审计。

严格的安全访问控制和管理员身份认证。

审计信息加密存储。

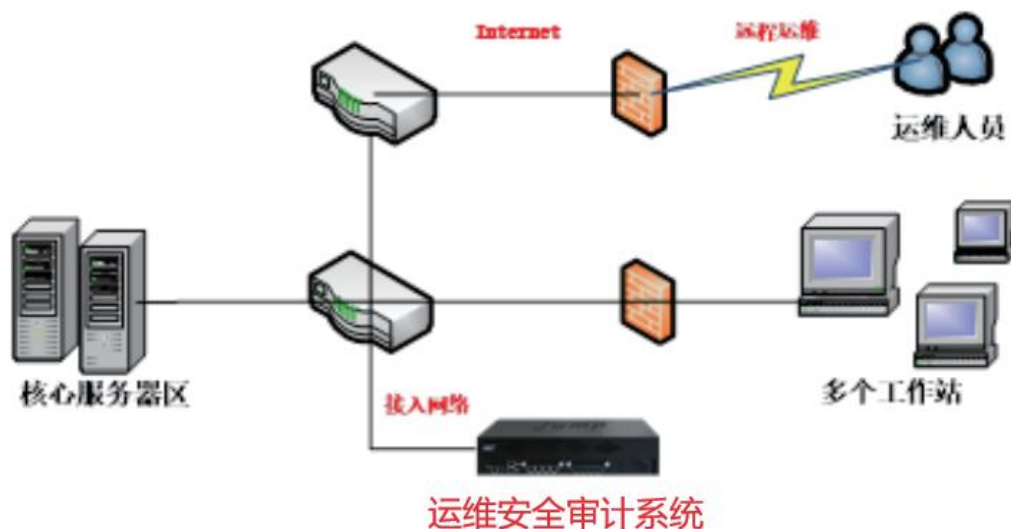
口令信息加密存储。

完善的审计信息备份机制。

完整全面的自审计功能。

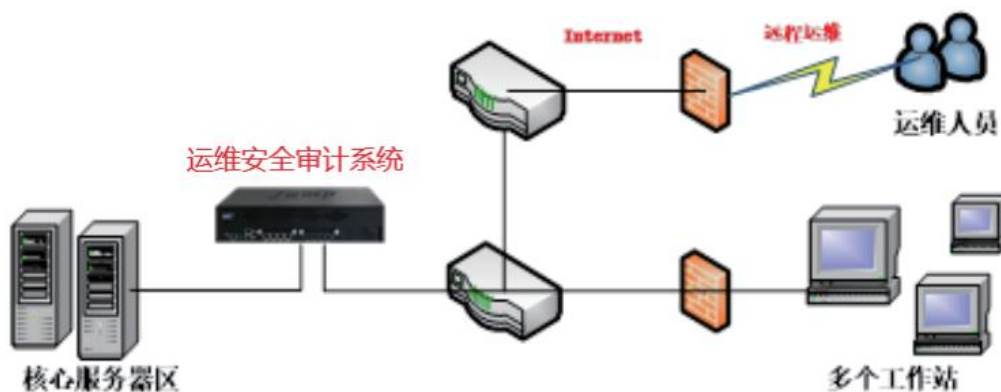
典型应用

单臂模式部署



单臂模式是目前应用最多的模式。华康安全运维管理系统只需要管理口接入到用户网络即可。在该模式下，通过华康安全运维管理系统访问IT基础服务资源的操作都将被详细地记录和存储下来，作为审计的基础数据。该部署不会对业务系统、网络中的数据流向、带宽等重要指标产生负面影响，无需在核心服务器或操作客户端上安装任何软硬件系统。

中间机模式部署



华康安全运维管理系统以中间机(串行)模式部署于网络交换机与核心服务器之间，所有与核心服务器交互的网络数据都会通过系统。



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

版权声明©2025力控，保留一切权利。BJ01/25-210-285



关注公众号



关注小程序