2022

适用范围：公开

产品白皮书

天玥运维安全网关 V6.0

运维堡垒机

适用范围：天玥 OSM 系列

精细控制合规审计

北京启明星辰信息安全技术有限公司

版权声明

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京启明星辰信息安全技术有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但北京启明星辰信息安全技术有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如有任何宝贵意见，请反馈：

信箱：北京市海淀区东北旺西路 8 号中关村软件园 21 号楼启明星辰大厦邮编：100193

电话：010-82779088

传真：010-82779000

您可以访问启明星辰网站：www.venustech.com.cn 获得最新技术和产品信息。

目录

1 运维安全管控的需求

1.1 特权帐号风险管理需求

企业内部资产承载着大量特权帐号，没有进行严格的权限划分与访问认证，管理人员无法进行有效管理，往往特权帐号掌握着企业核心数据，任何一个操作都可能导致核心数据的修改和泄露。特权帐号的滥用，让运维安全变得更加脆弱，也让责任划分和威胁追踪变得更加困难，需要解决以下问题：

1、需要建立帐号密码安全策略及技术体系，实现特权帐号密码定期改密；

2、需要实现对特权帐号进行权限最小化控制，并形成审计记录；

3、需解决帐号共享问题，将运维人员与特权帐号对应，准确定位安全事件。

1.2 系统共享帐号安全隐患

无论是内部运维人员还是第三方代维人员，基于传统的维护方式，都是直接采用系统帐号完成系统级别的认证即可进行维护操作。随着系统的不断庞大，运维人员与系统帐号之间的交叉关系越来越复杂，一个帐号多个人同时使用，是多对一的关系，帐号不具有唯一性，系统帐号的密码策略很难执行，密码修改要通知所有知道这个帐号的人，如果有人离职或部门调动，密码需要立即修改，如果密码泄露无法追查，如果有误操作或者恶意操作，无法追查到责任人。

1.3 内部人员操作的安全隐患

随着企业信息化进程不断深入，企业的业务系统变得日益复杂，由内部员工违规操作导致的安全问题变得日益突出起来。防火墙、防病毒、入侵检测系统等常规的安全产品可以解决一部分安全问题，但对于内部人员的违规操作却无能为力。

1.4 第三方维护人员安全隐患

企业在发展的过程中，因为战略定位和人力等诸多原因，越来越多的会将核心业务外包给设备商或者其他专业代维公司。如何有效地监控设备厂商和代维人员的操作行为,并进行严格的审计是企业面临的一个关键问题。严格的规章制度只能约束一部分人的行为，只有通过严格的权限控制和操作审计才能确保安全管理制度的有效执行。

1.5 违规行为无法控制的风险

管理员总是试图定义各种操作条例，来规范内部员工的网络访问行为，但是除了在造成恶性后果后追查责任人，没有更好的方式来限制员工的合规操作。而事后追查，只能是亡羊补牢，损失已经造成。

2 产品综述

2.1 产品简介

天玥运维安全网关 V6.0（以下简称天玥 OSM 系统）是一种管控和审计运维人员操作的网络安全设备。

管理员可以使用天玥 OSM 系统控制运维人员能运维哪些设备，执行哪些操作命令，避免运维人员非法或无意执行高危操作，并对运维人员的操作进行实时监控和事后审计。

运维人员通过天玥 OSM 系统做运维，不必记录设备的 ip 地址、用户名、口令等信息，也避免这些敏感信息的泄露，极大地方便了运维工作，提升运维效率。

天玥 OSM 系统对整个运维过程从事前预防、事中控制和事后审计进行全程参与。

事前预防：建立“自然人-资源-资源帐号”关系，实现统一认证和授权。

事中控制：建立“自然人-操作-资源”关系，实现操作审计和控制。

事后审计：建立“自然人-资源-审计日志”关系，实现事后溯源和责任界定。

2.2 系统组成

天玥 OSM 系统由管理模块、协议代理模块（应用发布模块扩展协议支持）组成。

- **管理模块**

管理模块为所有用户提供统一的身份认证登录入口。管理员用户可进行运维用户管理、设备及帐号管理、用户授权管理和运维审计管理等管理功能；运维用户通过管理模块进行资源单点登录等操作。

- **协议代理模块**

实现对主机、数据库、网络设备等资产维护过程中的协议数据包代理转发、操作行为记录及还原、高危/违规行为阻断等功能。

- **应用发布模块（可选）**

部署于 Windows Server 2008、Windows Server 2012、Windows Server 2016 服务器上，用于发布非标准协议或应用客户端，如 HTTP/HTTPS、Radmin、VMware client 等。可实现对应用客户端工具的调用、密码代填和操作审计功能。

3 产品功能介绍

3.1 单点登录

运维用户只需经过天玥 OSM 系统一次认证，通过返回的授权列表，直接访问目标资源，无须二次输入帐号和密码。运维用户只需要记住自己的天玥 OSM 系统登录帐号、密码即可，无需记忆繁多的目标资源 IP、帐号和密码信息。

3.2 身份认证

在信息系统的运维操作过程中，经常会出现多名维护人员共用设备（系统）帐号进行远程访问的情况，从而导致出现安全事件无法清晰地定位责任人。天玥 OSM 系统为每一个运维人员创建唯一的运维帐号（主帐号），运维帐号是获取目标设备访问权利的唯一帐号，进行运维操作时，所有设备帐号（从帐号）均与主帐号进行关联，确保所有运维行为审计记录的一致性，从而准确定位事故责任人，弥补传统网络安全审计产品无法准确定位用户身份的缺陷，有效解决帐号共用问题。

天玥 OSM 系统支持多种身份认证方式，并支持用户属性中手机号码和邮箱地址作为主帐号身份登录。

身份认证方式包括：

- 静态密码认证。
- USB-key 认证。
- 动态口令卡。
- 短信认证（短信网关标准：中国移动 CMPP2.0、中国联通 SGIP1.2 标准和中国电信 SMGP3.0）。

- 数字证书认证：吉大正元证书认证、北京数字证书认证。

支持外部协议扩展：Radius、LDAP、AD。

3.3 访问授权

天玥 OSM 系统通过基于角色的权限访问控制，实现细粒度授权与策略控制。

- 管理员可根据目标资源设置不同角色；
- 支持时间、命令、审批规则制定，并可与资源角色关联，实现不同运维用户访问资源遵从不同的控制策略；
- 支持限制 RDP 访问使用剪贴板、磁盘映射功能。

3.4 密码托管

天玥-OSM 系统支持对目标资源帐号的密码维护托管功能，支持类型：Linux、Unix、Windows（采用 RPC 方式）、AIX 以及数据库 Oracle、SqlServer、PostgreSQL、MySql、DB2、Informix 、SYBASE。

密码管理支持以下功能：

- 针对不同资源制定不同改密分组；
- 设定自动改密周期或者一次性改密；
- 支持随机不同密码、随机相同密码、手工指定密码等新密码设定策略；
- 改密结果自动发送至密码管理员邮箱；
- 改密结果高强度加密保护功能。

3.5 协议审计

天玥 OSM 系统能够对运维人员登录目标设备上进行的操作进行全程记录，包括字符协议（SSH、TELNET）、文件传输协议（FTP、SFTP）、数据库协议的所有操作命令的完整详细记录，图形协议（RDP、VNC）的完整操作图形记录。

天玥 OSM 系统能够以回放的形式重现运维人员对目标设备的整个操作过程，从而真正实现对操作内容的完全审计。

- 以 WEB 在线或离线方式视频回放重现运维人员对目标设备的所有操作过程。
- 支持从特定操作指令开始进行定位回放。
- 支持倍速播放、拖动、暂停、停止、重新播放等播放控制操作。
- 支持图形协议（RDP、VNC）空闲操作过滤，节省磁盘空间。

3.6 监控与回放

对于所有远程访问目标主机的会话连接，天玥 OSM 系统均可实现操作过程同步监视，运维人员在远程主机上做的任何操作都会同步显示在管理人员的监控画面中，管理员可以随时手工中断违规操作会话。

3.7 告警与阻断

天玥 OSM 系统支持根据已设定的访问控制策略，自动检测日常运维过程中发生的越权访问、违规操作等安全事件，系统能够根据预设规则进行自动的告警或阻断违规的操作行为。

- 阻断方式支持：断开会话、忽略指令。
- 告警方式支持：以 SYSLOG、邮件、SNMP 实时发送告警信息。

3.8 二次审批

1、命令审批：支持根据需求对特殊指令操作进行二次审批功能，运维人员操作过程中触发命令策略，需要得到审批员的审批后才能继续执行后续操作。

2、登录审批：可定制审批规则与资源角色关联，对运维人员访问资源制定登录审批策略，需要得到审批员的审批后才能继续执行后续操作。

1.1 审计报表

支持按日、周、月为周期自动生成周期性报表，报表格式支持 CSV 和 HTML 格式导出。

1.2 帐号稽核

天玥 OSM 提供支持僵尸、幽灵、孤儿帐号分析，以降低企业安全风险

- 检测僵尸帐号：周期内登录次数低于阈值的用户帐号和资源帐号。
- 检测幽灵帐户：天玥 OSM 中未托管但又真实存在的的资源帐号。
- 检测孤儿帐户：没有建立授权关系的用户帐号和资源帐号。

1.3 工单管理

支持管理员下发工单，授权运维人员有权限在指定时间内访问指定的资源；

支持运维用户主动申请访问权限的工单，管理员审批通过后即可登录资源进行运维。

1.4 自动运维

天玥 OSM 面向运维人员提供网络资源配置自动备份、命令自动执行功能。

1.5 IPV6 支持

IPv6 网络环境下，支持网络配置管理与运维。

1.6 高可用性

系统支持双机（主-备）模式，可自动备份配置。

1.7 系统安全

管理模式采用 HTTPS 方式进行远程安全管理。

系统自身 HTTPS 证书签名支持高强度算法。

支持网口聚合功能。

4 产品优势

4.1 运维协议全面性

天玥 OSM 支持多种运维访问协议，能够充分满足日常运维需要。

- 字符协议：SSH、TELNET。
- 图形协议：RDP、VNC。
- 文件传输协议：FTP、SFTP。
- 数据库访问：Oracle、SQL Server、DB2、Sybase、Informix、Teradata、MySQL、PostgreSQL。

- 通过应用发布进行协议和运维工具扩展，支持 HTTP/HTTPS、X11、Radmin、VMvare client 客户端等。

4.2 认证方式多样性

天玥 OSM 系统包括多样认证方式，其中内置动态口令认证系统，从而使用户实现无需额外购置动态口令牌认证系统即可完成用户口令动态认证模式。

天玥 OSM 系统支持对不同用户设置不同认证方式组合的双因素认证，更具灵活性。

认证方式包括：静态口令认证、USB-key 认证、动态口令卡、短信认证（支持短信中间表和短信网关标准，短信网关包括中国移动 CMPP2.0、中国联通 SGIP1.2 标准和中国电信 SMGP3.0）、数字证书认证（包括吉大正元证书认证、北京数字证书认证）、Radius 认证、LDAP 认证、AD 域认证

4.3 审计效果精细化

- 支持字符协议和文件传输协议的协议审计，审计详细的操作语句和操作语句的执行结果。
- 支持 RDP、VNC 图形操作过程中键盘输入操作记录、鼠标点击行为记录和窗口标题审计。
- 数据库协议深度解析、数据库返回行数记录。
- 支持通过应用发布实现数据库、字符协议、文件传输协议命令和录像的双重审计效果。

4.4 管控方式严格性

天玥 OSM 系统提供严格的管控方式以保证运维过程的规范性。

- 命令限制与复核：对于高危命令实现实时告警或阻断，对于特别重要的命令实现多人审核。
- 应用发布防跳转：防止通过应用发布服务器进行跳转登录未授权资源，进行 http/https 访问过程时运维人员仅允许访问授权地址，保证运维的规范性。
- 运维帐号 IP、MAC 限制：通过绑定用户 IP/MAC 地址，防止用户在网络上未授权的终端进行运维操作。

4.5 操作使用便捷性

天玥 OSM 系统提供多种功能以保证运维过程的自动和快捷性，本地客户端无需安装 Java 控件，即可实现单点登录。

- B/S 运维模式：支持 IE、谷歌浏览器、Firefox 浏览器，无需安装 Java 控件。
- C/S 运维客户端模式：用于运维人员通过运维客户端登录进行运维操作，整个运维过程不依赖任何 Active 或 Java 控件。
- SSH/RDP 直连菜单模式：为运维用户提供 SSH/RDP CLI 工具直连模式，通过认证后进行资源的访问。支持 SecureCRT，Mstsc 工具。
- 支持以普通管理模式登录网络设备或主机并自动切换到特权模式。
- 支持从 AD 域抽取组织机构和用户帐号，方便快速建立组织机构和用户帐号。
- 支持资源自动发现和添加，便于快速添加资源。
- 资源批量登录：支持 TELNET、SSH 协议使用 SecureCRT 工具批量登录目标资源，避免进行多次连接的重复工作量。
- 设备自动改密：支持对目标设备自动定期修改密码，特别是数据库协议（包括 Oracle、SQL Server、DB2、Sybase、Informix、MySQL、PostgreSQL）。

4.6 自动运维高效性

天玥 OSM 系统支持面向运维人员实现批量化周期自动备份网络设备配置，提高网络管理人员的工作效率。

天玥 OSM 系统支持面向运维人员实现批量登录 Linux 类资源，并可自动执行命令，得到反馈信息，提高运维人员的工作效率，实现高效运维。

4.7 部署方式灵活性

天玥 OSM 系统支持单机、双机、分布式部署多种部署方式，并支持 NAT 和网口聚合方式，适应多变业务场景。

- 分布式部署：

  支持添加一台或多台协议代理服务器，分担审计中心性能压力，便于提高整体性能；

  并支持限定不同的协议代理服务器节点访问不同的资源；

  多协议代理服务器节点可访问相同资源时实现自动负载均衡；

  审计中心集中管理配置和日志信息；

- 网口聚合功能：主备模式，防止链路单点故障；负载均衡模式，提高链路带宽；
- 支持 NAT 地址映射部署：通过映射后的 IP 地址访问堡垒机进行管理和运维操作，

  支持从多个映射地址访问，适用于内外网隔离的复杂网络环境。

5 产品部署

天玥 OSM 系统采用物理旁路方式部署，不需改变现有网络结构，只需确保天玥 OSM 系统和应用发布服务器与被管资源以及用户终端维护区域网络可达即可。

根据用户业务需要，标准部署方式可分为单机、双机和分布式部署。

5.1 单机部署

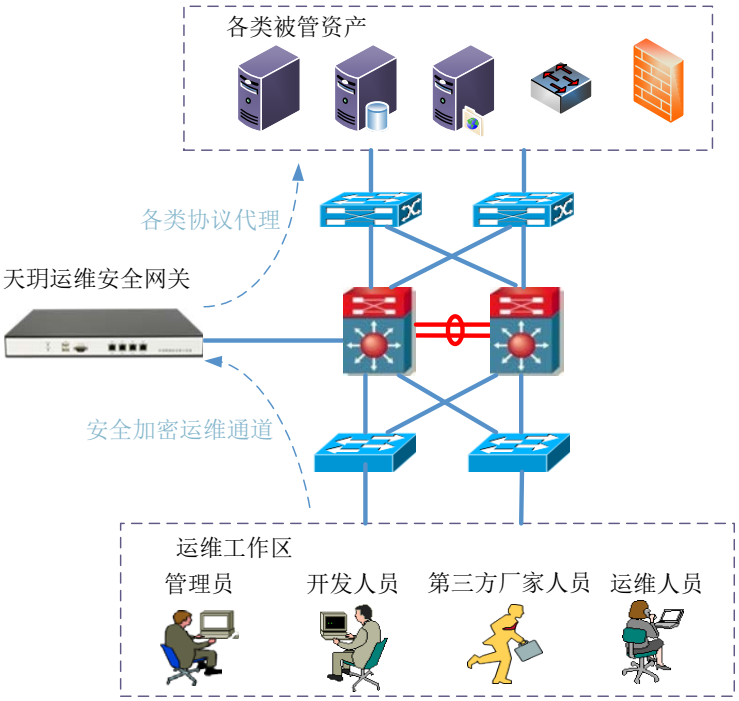

图 5.1 单机部署

如图所示，天玥 OSM 系统旁路方式部署于网络中，无需对网络结构进行任何调整。部署天玥 OSM 系统后，运维人员直接访问天玥 OSM 系统的对应端口，建立安全加密的数据通道，然后再通过天玥 OSM 系统发起到服务器对应服务的访问，运维人员无需直接访问服务器，从而进一步加强内部服务器的安全性。

5.2 双机部署

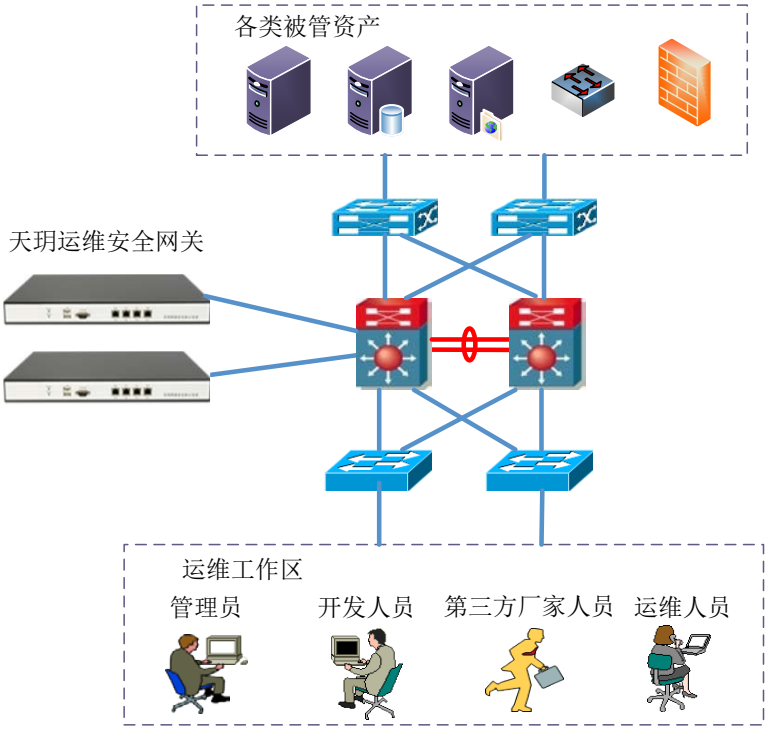

图 5.2 双机部署

如图所示，天玥 OSM 系统支持 HA 双机热备部署，以避免单点故障隐患，最大程度满足运维的可靠性和连续性。HA 双机热备部署由两个节点组成，分为主机节点和备机节点，主备之间通过组播进行主备状态监测，并配置同步，主机节点一旦断开，备机节点会立刻启动，无需人工干预，从而实现业务的不间断运行。

5.3 分布式部署

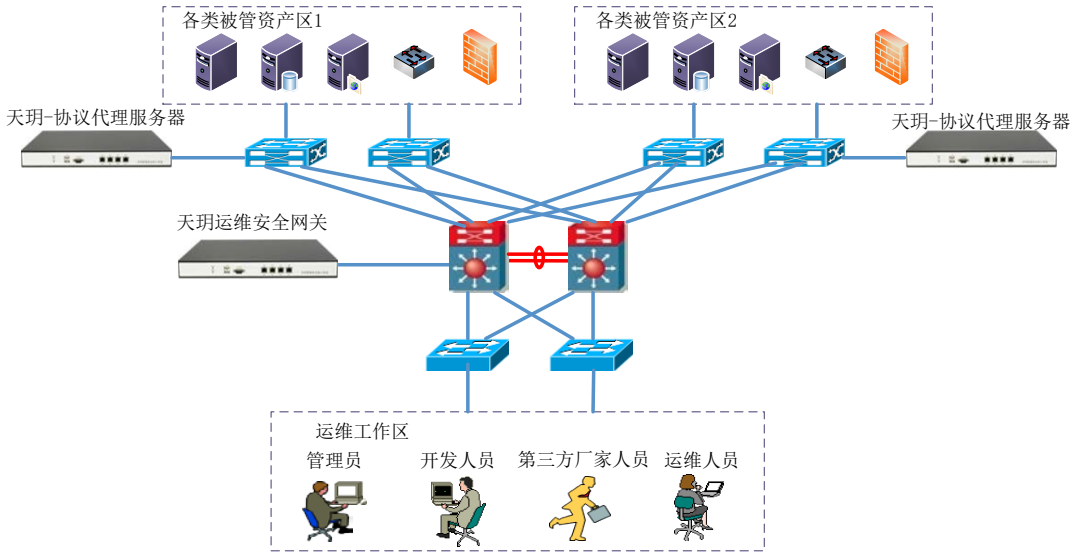

图 5.3 分布式部署

如图所示，天玥 OSM 系统支持分布式部署，把天玥 OSM 系统切换至协议代理服务器模式部署在各个合适的网络节点，天玥 OSM 系统主服务器部署在上层中心交换网络中。通过天玥 OSM 系统主服务器管理界面对所有协议代理服务器进行统一的管理，运维用户运维操作产生的协议代理行为会通过负载均衡的方式分配到协议代理服务器上，同时各协议代理服务器实时传输审计日志到天玥 OSM 系统主服务器。

6 产品价值

6.1 完善内控内审，满足合规要求

目前，越来越多的单位面临一种或者几种合规性要求。比如，在美上市的中国移动集团公司及其下属分子公司就面临 SOX 法案的合规性要求；而商业银行则面临 Basel 协议的合规性要求；政府的行政事业单位或者国有企业则有遵循等级保护的合规性要求。

天玥-OSM 提供一种完备的审计方案，有助于完善组织的 IT 内控与审计体系，从而满足各种合规性要求，并且使组织能够顺利通过 IT 审计。

6.2 简化运维管理，提高运维效率

天玥-OSM 系统对帐号和资产进行统一管理，规范简化运维流程。提供多种运维操作方式以满足各种不同使用习惯。自动便捷的使用体验提供整体运维效率。

6.3 控制运维风险，防止数据泄露

天玥-OSM 系统基于统一认证、集中管理、规范运维操作行为，对运维操作和数据流转过程做到严格的控制和记录，最大程度控制运维风险。

7 总结

天玥运维安全网关 V6.0 能够对运维人员维护过程进行全面跟踪、控制、记录、回放；支持细粒度配置运维人员的访问权限，实时阻断违规、越权的访问行为，同时提供维护人员操作的全过程的记录与报告；系统支持对加密与图形协议进行审计，消除了传统行为审计系统中的审计盲点，是 IT 系统内部控制最有力的支撑平台之一。