運維管理平台

GATEKEEPER

Server connection operation audit log

全球系統整合股份有限公司
Global System Integration CO., LTD

資訊安全—操作稽核是目前最被忽略

機房不管是共構或單一，操作記錄如何追蹤？

面臨安全風險

隨著 IT 建設的不斷深入和完善，電腦軟硬體系統的運行維護已經成為了各行各業各單位管理者和資訊服務部門普遍關注和不堪負荷的問題。由於這是隨著電腦資訊技術的深入應用而產生的，因此如何進行有效的 IT 運維管理，這方面的知識積累和應用技術還剛剛起步。對這一領域的研究和探索，將具有廣闊的發展前景和巨大的現實意義。

大中型企業和機構紛紛建立起龐大而複雜的 IT 系統，IT 系統的運營、維護和管理的風險不斷加大。運維管理安全風險是指運維用戶在運維操作中引起的風險。這裡由於變更設計不完善、誤操作、越權操作、惡意操作及代操作等因素。因運維管理一般是採用特權用戶進行操作，所以其操作風險是非常大。目前大多用戶採用分權雙人、各種管理制度等 (或內控) 方式來規避或降低 ,但實際運行中由於制度落實等問題，無法做到全面的控制 運維安全仍然存在很大的風險。針對目前運維管理，主要存在以下幾種風險。

由於 IT 運維操作的複雜度，致使我們無法知道運維用戶在過去和現在都對設備進行了哪些操作，這些操作是否會對設備及業務造成影響；而一旦出現問題，企業 (或公家單位)IT 部門也無法追溯到是誰在什麼時候以及做了哪些操作導致的問題；其實企業 (或公家單位) 都有一定的制度來控制設備帳號以及運維使用者許可權，但由於沒有技術保障，很難做到完全的執行。

IT 系統稽核是控制內部風險的一個重要手段，尤其個資法通過之後，各單位更加重視資料保密性及安全性，但 IT 系統構成複雜，操作人員眾多，如何有效地對其進行稽核，是長期困擾各組織的資訊科技和風險稽核部門的一個重大課題。而由於資訊系統的脆弱性、技術的複雜性、操作的人為因素，企業 (或公家單位) 目前無法實現對各類系統及網路設備的運維使用者操作記錄的即時監控和稽核；同時雖然企業 (或公家單位) 能定期修改設備的密碼，但由於設備的交叉管理，無法確保設備密碼的安全性，也就無法有效的保護企業 (或公家單位) 的資訊安全。

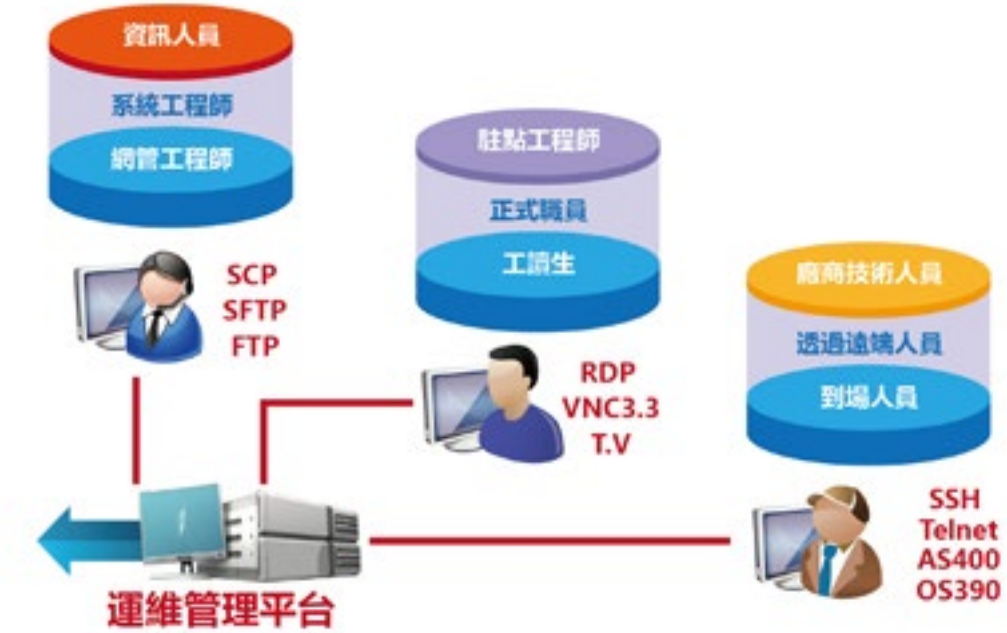
GateKeeper 用途說明

GateKeeper 可對主機、伺服器、網路設備、安全設備等的管理維護進行安全、有效、直觀的操作稽核，對策略配置、系統維護、內部連結等進行詳細的記錄，提供細微性的稽核，並支援操作過程的全程重播。GateKeeper 彌補了傳統稽核系統的不足，將運維稽核由事件稽核提升為內容稽核，並將身份認證、授權、管理、稽核等有效性的結合，保證只有合法用戶才能使用其擁有運維許可權的關鍵資源。GateKeeper 為組織在 IT 操作風險控制、內控安全和合規性等方面提供一套完善、有效的稽核手段。

GateKeeper 支援 Telnet、FTP、SSH、SFTP、RDP（Windows Terminal）、Xwindows、VNC、AS400、OS390、HTTP、HTTPS 等多種通信協定，支援 IBM AIX、Digital UNIX、HP UNIX、SUN Solaris、SCO UNIX、LINUX、WINDOWS 等多種作業系統。可廣泛應用於金融、政府、電信、證券、郵政、財稅、海關、交通、軍警、教育、高科技產業、醫院等安全需求較高的行業。

運維管理平台—在機房主機運作上能做什麼？

運維平台—運維用戶主要適用對象



集中存取控制

身份管理和認證：

支援運維用戶 Local 認證、LADP 認證、AD 域認證、Raduis 認證、POP3 認證方式。支援密碼強度、密碼有效期、帳密嘗試鎖定、用戶啟動等安全管理功能。支援用戶分組管理。支援使用者資訊匯入匯出，方便整批處理。

授權：

系統提供依據使用者、運維協定、目標主機、運維時間段、運維用戶端 IP 等組合的授權功能，實現細微性授權功能，滿足用戶實際授權的需求。提供依據用戶到資源的授權。提供依據用戶組到資源的授權。提供依據用戶到資源組的授權。提供依據用戶組到資源組的授權。
（資源是指主機上的某一種服務，一個主機可能有多個資源。比如主機 A 有 RDP，FTP，VNC 等，這三個資源可以分別進行授權和分組，當然也可以和其他主機的資源進行組合。）

運維平台架構 (Proxy) 說明

稽核功能

事中稽核與控制：

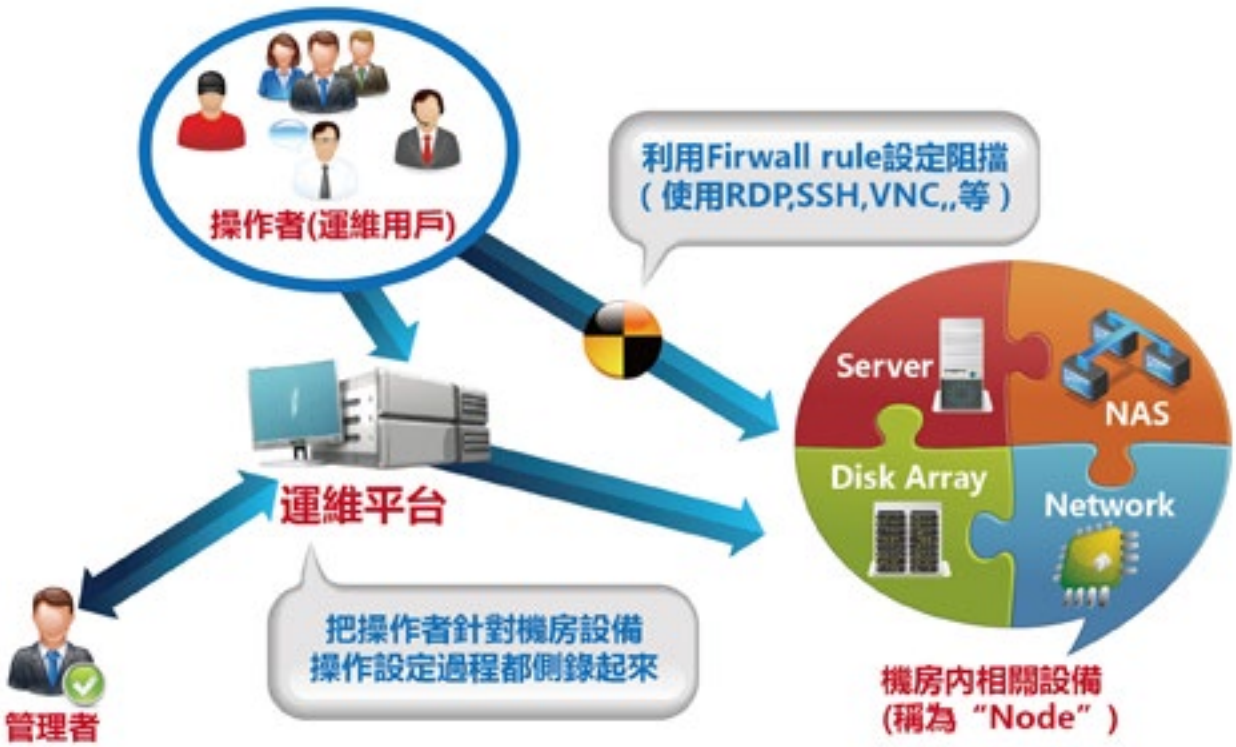
1、即時監控：

監控正在運維的連接，資訊包括運維使用者、運維用戶端位址、資源位址、協定、開始時間等。提供線上運維操作的即時監控功能。針對命令交互性協定可以圖像方式即時監控正在運維的各種操作，其資訊與運維用戶端所見完全一致。

2、違規操作即時告警與阻斷：

針對運維過程中可能存在潛在操作風險，GSI GateKeeper 根據使用者配置的安全性原則實施運維過程中的違規操作檢測，對違規操作提供即時告警和阻斷，從而達到降低操作風險及提高安全管理與控制的能力。非字元型協定的操作能夠即時阻斷，字元型協定的操作可以通過命令列配置進行規則匹配實現告警與阻斷。提供使用者可配置的告警規則。在具有自動登錄功能的 GSI GateKeeper 上，可實現告警規則與後台資源的帳戶級別進行綁定，針對不同使用者實施不同的規則，從而提供更細微性的操作控制。告警動作支援連接阻斷、稽核平台告警、郵件告警、Syslog 告警、SNMP TRAP 告警等。

運維平台—“它”是什麼東西？



事後稽核與報表：

1、完整記錄網路連接過程：

系統提供運維協定 Telnet、FTP、SSH、SFTP、RDP、 Xwindows、VNC、SCP、HTTP、HTTPS 、AS400、OS390、TeamView(VDH 應用，須提供 win 2003 server) 等網路連接的完整連接記錄，完全滿足內容稽核中資訊百分百不遺漏的要求。連接資訊包括運維使用者、運維位址、後台資源位址、資源名、協定、起始時間、終止時間、流量大小資訊。

2、詳盡的連接稽核與重播：

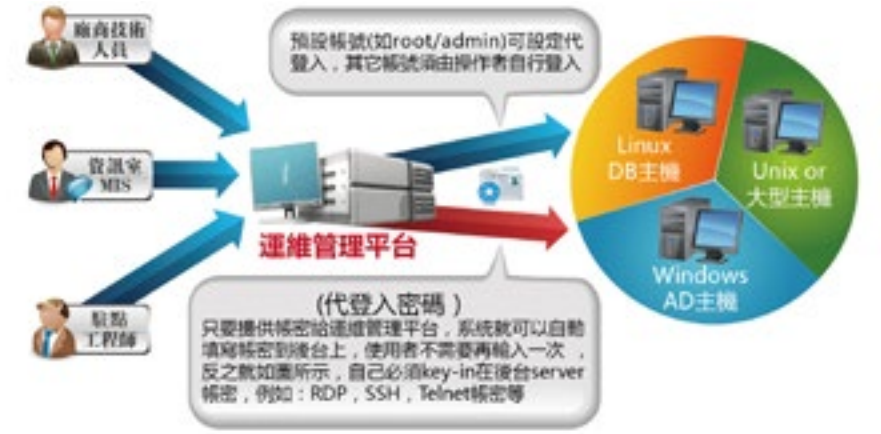
運維操作稽核以連接為單位，提供當日和條件查詢定位。條件查詢支持按運維用戶、運維地址、後台資源位址、協定、起始時間、結束時間和操作內容中關鍵字等組合方式。提供圖像形式的重播，真實、直觀、可視地重現當時的操作過程。重播提供快放、慢放、拖拉等方式，方便快速定位和查看。針對命令對話模式的協定，提供按命令進行定位重播。針對 RDP、Xwindows、 TeamView、 VNC 協定，提供按時間進行定位重播。

3、完備的稽核報表功能：

GSI GateKeeper提供運維人員操作，管理員操作以及違規事件等多種稽核報表。提供日常報表，包括今日連接、今日稽核、使用者資訊、資源資訊、許可權資訊、規則資訊、管理員角色資訊等報表。提供連接報表，可根據使用者選定時間、使用者、資源形成連接報表。告警報表，可根據告警類別、級別、資源、運維使用者、協定、時間等條件形成報表。綜合統計報表，可根據時間、資源、使用者等條件形成綜合統計報表，報表中包括概要資訊、每個使用者操作資訊、每個資源被操作資訊等。

運維用戶—可選擇多種方式連接運維平台

代登入密碼（不想讓操作者知道密碼時）



線上審核機制（操作者要連線主機時，須線上申請）

系統功能規格說明

系統型號	GKP-10	GKP-30	GKP-50	GKP-100	GKP-200	GKP-300
支持 Node 數	10	30	50	100	200	300
字符連線數	50	60	300	500	800	1,000
圖形連線數	20	30	80	100	200	300
建議伺服器等級						
CPU / Core 數以上	1/2	1/2	1/4	1/4	2/8	2/8
RAM(可用空間以上)	2G	3G	4G	8G	12G	16G
網路介面 Giga(TX/SX/LX)	1	1	1	1	1	1
工作模式						
旁路模式 (Proxy)	√	√	√	√	√	√
H.A 備援 (A/S)	√	√	√	√	√	√
支援協定						
SSH , Telnet , SCP , SFTP , FTP , AS400	√	√	√	√	√	√
X windows , OS390	√	√	√	√	√	√
RDP , VNC , HTTP , HTTPS	√	√	√	√	√	√
儲存方式						
Local HDD(建議)	250G	320G	500G	1T	2T	2T
外部 NAS(自備規劃)	√	√	√	√	√	√
身份認証 / 網路管理						
稽核分析	√	√	√	√	√	√
記錄查詢 (用戶 , 時間 , 指令 , 主機 , 資源等)	√	√	√	√	√	√
線上審核及事先審核機制	√	√	√	√	√	√
帳號托管	√	√	√	√	√	√
異動連線告警 (SSH , Telnet)	√	√	√	√	√	√
郵件通知機制	√	√	√	√	√	√
AD/LDAP 組織整合	√	√	√	√	√	√
AD/LDAP/POP3/Radius	√	√	√	√	√	√
帳號機主機比對	√	√	√	√	√	√
Web 中文介面管理	√	√	√	√	√	√
四權分立管理機制 (Role)	√	√	√	√	√	√

GKP 系列產品

GKP-10/30/50/100/300 系列 運維管理平台
Node : 10 , 30 , 50 , 100 , 200 , 300
字符連線數 : 50 , 60 , 300 , 500 , 800 , 1000
圖形連線數 : 20 , 30 , 80 , 100 , 200 , 300

授權經銷商

全球系統整合股份有限公司
Global System Integration CO., LTD
高雄市新興區民權一路251號10F之3
TEL:+886-7-2260326
FAX:+886-7-2234699
全球資訊網 : http://www.nethi.com.tw