SOOP-CLM
集中式日誌管理平台

Service-Oriented Operation Portal - Centralized Log Management

產品定位

SOOP-CLM 是一個高性價比的企業級集中化日誌管理解決方案，由於它吃到飽授權特色，可以集中收容多樣性的日誌來源與不同的日誌格式，並進一步分析、關聯、儲存及視覺化日誌資料。不但一次滿足政府法令及稽核等需求，也是企業面對資訊安全與大數據時代的堅強後盾，更可以結合其他第三方解決方案，節省整體擁有成本，增加企業競爭力。

產品六大特色：

1 強大的集中收容能力，便於高效率查找及降低資料流失風險

可集中收容眾多裝置上不同格式的日誌資料，透過內建的多樣解析模組分析關聯所收容的各種日誌資料；提供關鍵字查詢並視覺化相關資訊，平均百萬資料秒級回應；若結合 Data Queue 模組，作為蓄洪池之用，避免突發大量流量衝擊下，資料遺失風險；亦可將長期歷史資料壓縮儲存或整合 Hadoop 作為資料倉儲之用。

2 功能完整的日誌管理解決方案，易於操作上手及符合稽核管理要求

支援 AD/LDAP 及 OIDC 認證方式，具備密碼管控機制，嚴格的 Role-based access control 控管存取權限，內建 Document Level Security 以符合 ISO 27001 要求，保護日誌資料且具不可竄改性，並可留存歷史資料以符合 ISO 27001 與 PCI DSS 等日誌稽核項目，達到法規遵循及企業稽核標準；提供簡易人機操作介面，可於 Web UI 上設定告警、報表排程和日誌解析規則等日誌管理功能，降低學習曲線；內建多樣視覺化模組，或運用時間過濾功能和拖拉式自定義儀表板功能，快速滿足不同視覺化需求。

PiExtract 信研科技股份有限公司

MAIL : support@piextract.com

3 穩定可靠的分散式架構設計，有效降低維護負擔，避免單點失效風險

去中心化架構的分散式運作叢集設計 (Active-Active)，內建 Load Balance 機制，支援雲端、地端或混合雲架構，輕鬆達到簡易擴充，高可用度的目標；透過 SOOP-CLM 的自我監控及健檢功能，維運人員可輕易的掌握系統平台當前狀態，當系統平台運作遭遇瓶頸時，可協助迅速排除異常，大幅降低管理難度；內建防呆機制，可阻擋一般性不當之人為操作或管理疏忽。

4 智能告警機制，提供真實的趨勢分析及反映真實狀況

SOOP-CLM 內建的動態閾值透過先進的演算法，自動依據過去的歷史數據，為不同時段定義更貼近現實的閾值，協助判斷是否發生異常，有效提升網路與資安告警的精準度，降低發送 False Alarm 的機率，協助用戶第一時間察覺異常，同時加速排除作業，提升系統可靠度，進一步推升使用者滿意度，達到早期告警、快速定位、高效維運的目標，如此一來，即可快速、精準定位異常範圍，有效減少排除異常時間，降低管理成本，提升維運效率。

5 小中心大周邊設計理念，整合其他第三方解決方案，擴大投資效益

提供多種 API，方便用戶整合或開發各種面向的第三方應用服務；在 IT 維運環境中，整合多種監控工具數據視覺化呈現，作為 NOC 之用；串接大數據平台，可挖掘其中商業價值，擴大投資效益；整合 AIOps 工具，搭配 RPA 等機器人流程自動化工具，進行主動修復及預測分析等應用，讓 IT 管理更具智慧化，加速企業數位轉型；結合 SOC 等資安軟硬體產品，不但可作為資安聯防一員，並可留下數位軌跡，以利數位鑑識查找，輔助資安政策制定。SOOP-CLM 的高整合性能發揮各產品的最大效益，節省整體擁有成本，增加企業競爭力。是企業在面對資安風險和 AI 時代的最佳選擇。

6 高性價比的計價方式，輕鬆擁有無後顧之憂

免費支援新設備的日誌解析處理，不必煩惱往後日誌平台維護支出增加；授權不限流量 / EPS / 容量 / CPU / Memory / 日誌來源設備數 / 日誌量 / 操作使用者數量，透過擴充硬體資源或節點方式，彈性部署節省使用成本；不斷推陳出新的日誌應用及插件，將投資效益發揮到最大；內建多樣化應用服務，大幅縮減客製化開發的時程及負擔；基於開源具備高自由度及在地支援，有效減少未來轉換成本和使用風險；國外官方維護及本地多方弱掃，雙重保障確實降低資安疑慮；客戶橫跨政府 / 金融 / 電信，產品經多方檢驗，品質成熟穩定有保障。

成功案例 – IT 日常維運

利用 SOOP-CLM 集中收集 400＋台伺服器，200＋台網路設備之日誌資料，每日收集超過 150GB 的日誌資料。
當 SOOP-CLM 發現系統狀況異常時，SOOP-CLM 會主動發出通知，讓維運人員可即時掌握系統狀態。

導入 SOOP-CLM 的效益

快速查詢，降低問題查找時間

1. 在單一平台透過關鍵字查詢相關日誌資料，交叉比對，縮短服務恢復時間：2 小時 => 0.5 小時。
2. 將日誌視覺化呈現，可一眼看出相關項目是否異常，以便維運人員做出對應的處理。

藉由日誌集中管理，強化日常維運效率

監控『異常登入行為』、『單一 IP 流量大幅增加』及『不被允許的設定變更』等等行為，強化管理。

成功案例 – 資安 / 稽核應用 ISO 27001

符合資訊安全稽核需求

符合 ISO 27001 日誌稽核規範

A.12.4 存錄與監控 (目標：紀錄事件與生成證據)

(1) A.12.4.1 事件存錄

事件日誌係紀錄使用者活動、異常、錯誤及資訊安全事件，應產生並保留且定期審查。

(2) A.12.4.2 日誌資訊的保護

應保護存錄設施與日誌資訊，不受竄改與未經授權的存取。

(3) A.12.4.3 管理者與操作者日誌

系統管理者與操作者的活動應加以存錄、保護並定期審查。

A.12.4 存錄與監控

導入 SOOP-CLM 的效益

建構 ISO 27001 稽核儀表板，提升資訊安全

清楚呈現所有資訊，協助客戶符合 ISO 27001 日誌稽核項目，以提升整體資訊安全性。

日誌統一管理，簡化稽核流程

1. 大幅提升管理效率、減少稽核人力與時間 (每季稽核花費時間由 10 天縮短至 10 分鐘內完成)
2. 降低手動稽核可能造成的失誤，更可以即時追蹤違反資安的事件。

維運參考依據

1. 可針對特定事件進行關鍵字告警 (例如深夜 root 登入系統事件)，定時產出報表。
2. 可透過稽核報表來制定流程或管理的改善計畫。

成功案例 – 日誌減量應用

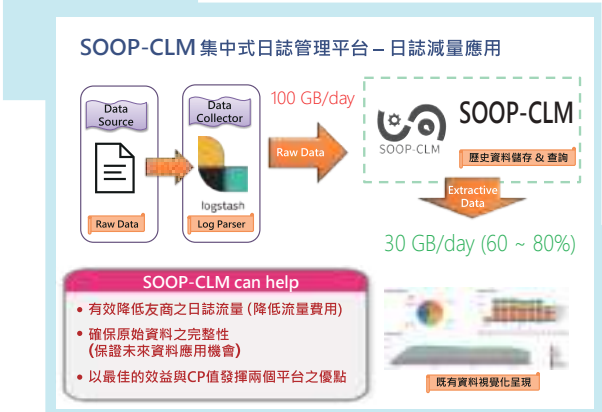
將 Raw Data 收集至 SOOP-CLM 中，確保原始資料之完整性，再透過 SOOP-CLM 過濾並計算出友商所需的資料，有效降低友商日誌流量。

導入 SOOP-CLM 的效益

保障既有投資，且大幅降低軟體授權費用

將日誌量減量 70% 後，僅將有使用到的日誌資料導入友商，以既有的資安事件開單，及資料視覺化儀表板呈現，不僅保障既有投資，更有效降低友商之日誌流量，降低每年支付之流量費用。

SOOP-CLM 收集全部日誌資料，維持日誌資料完整性，以利資料稽核及查詢。



日誌擴充收集不受限

日誌收容無流量限制，可完整收集突發性事件所產生之大量日誌資料及新設備日誌，確保原始資料之完整性 。

成功案例 – DB Audit Log

利用 SOOP-CLM 集中收容不同 DB 之操作行為，完整監控資料庫之狀態。

導入SOOP-CLM的效益

整合跨平台 DB Audit Log 資料

透過單一平台，整合不同種類之 DB Audit Log 資訊，讓維運人員不用維運多套 DB Audit 工具，僅須透過 SOOP-CLM 就可查閱所有 DB 之 Audit Log，並設定相關視覺化圖表。

完整記錄 DB 行為軌跡

利用 SOOP-CLM 收集 DB Audit Log，完整記錄所有 DB 行為軌跡，例如 DB 活動之時間、來源、使用者、SQL 指令等細節；這些資料除可用於稽核應用外，亦可作為後續分析之用。

即時收集，即時發現 DB 異常行為

維運人員可自行定義及設定 DB 異常行為規則，當 SOOP-CLM 偵測到 DB 異常活動時（如異常時間的存取行為，大量異常的資料存取紀錄等 ），相關維運人員可即時收到 SOOP-CLM 通知並處理。

當問題發生時，維運人員可透過 SOOP-CLM 提供之資料視覺化儀表板快速查找相關日誌紀錄，有效減少問題處理時間確保資料庫安全。

內建 Dashboard 及報表

OS

ESXi　Windows　Linux

事件相關
1. 事件級別數量趨勢圖
2. 事件級別分佈圖
3. 設備收容台數
4. 事件級別統計 (Information、Warning 等)
5. 設備收容台數

登入相關
1. AD 帳號鎖定統計
2. 登入成功 / 登出 事件總數
3. 登入成功 來源 IP / 登入帳號 事件統計及趨勢
4. 登入失敗 來源 IP / 登入帳號 事件統計及趨勢

排程相關
1. 排程 Audit 事件分佈圖及趨勢 (更新、刪除、停用、建立)
2. 各種排程日誌 (刪除、啟用、停用、更新)

開 / 關機相關
1. 關機時間紀錄
2. 開 / 關機分佈圖
3. 異常關機統計

效能監控
1. CPU、Memory、Disk、Top Process、Disk I/O、Network Traffic

網路設備

Flow - Base

1. Services、Autonomous Systems (如 Google、AWS、Yahoo 等)、IP Version 及 Protocols 等統計圖表
2. Top 10 Applications 統計分佈圖 (如 SSL、Gmail、Facebook 等)
3. Applications 流量圖
4. 來源 IP / 目的 IP 分佈圖
5. flow 流量圓餅圖 (Clients 以及伺服器)
6. Geo IP 流量圖 (國家、城市、Server 與 Client 流量、Service 流量、Client 位置、Server 位置)
7. 來源 / 目的 Autonomous Systems 趨勢圖 (流量、封包數)
8. Ingress / Egress Interfaces 趨勢圖 (流量、封包數)
9. Protocols / VLANs 圓餅圖 (流量紀錄)
10. Protocols / VLANs 趨勢圖 (流量、封包數)

Fortinet　Checkpoint　Palo-Alto

事件相關
1. 事件級別數量趨勢圖
2. 事件級別分佈圖
3. 設備收容台數

網路設備 Config 異動相關紀錄

登入相關
1. 登入成功 / 登出 事件總數
2. 登入成功來源 IP / 登入帳號 事件統計及趨勢
3. 登入失敗來源 IP / 登入帳號 事件統計及趨勢

Policy Rule 異動相關
1. Move Policy
2. Edit Policy
3. Delete Policy
4. Add Policy

Policy Rule Action
1. Deny
2. Allow
3. Close
4. Timeout

F5　Cisco

事件相關
1. 事件級別數量趨勢圖
2. 事件級別分佈圖
3. 設備收容台數

登入相關
1. 登入成功 / 登出 事件總數
2. 登入成功 來源 IP / 登入帳號 事件統計及趨勢
3. 登入失敗 來源 IP / 登入帳號 事件統計及趨勢

Config 異動相關紀錄

Middleware

DB

登入相關
1. 登入成功 / 登入 事件總數
2. 登入成功 來源 IP / 登入帳號
   事件統計及趨勢
3. 登入失敗 來源 IP / 登入帳號
   事件統計及趨勢

服務啟動紀錄

Audit Log

有別於市面上大部分的日誌集中收集平台授權方式，SOOP-CLM 授權方式為訂閱制，授權不限流量，由硬體大小決定可收容的日誌多寡！也就是說您不用再為每年日誌收容的高額流量授權費煩惱了，選擇 SOOP-CLM 可以讓您放心地進行全面的日誌收集！

內建支援之設備及系統清單

網路設備

Cisco
N9K-C93108TC-EX、ASR1002X-5G-K9
Cisco Nessus7010、1841、1721
C3900、C1900、3925、2821、
N9K-C9336PQ、C6509、CT3504
C2950 (WS-C2950G-24)
C2960 (WS-C2960-48PST-L、
WS-C2960-24TT-L、WS-C2960-24PC-L、
WS-C2960-48TC-L)
C2960G (WS-C2960G-24TC-L)
C2960X (WS-C2960X-48TS-L、
WS-C2960X-24TS-L)
C2960S (WS-C2960S-24TD-L、
WS-C2960S-48TD-L)
C3560G (WS-C3560G-48TS)
C3750G (WS-C3750G-24TS-1U)
C3750X (WS-C3750X-48P、WS-C3750X-48)
C3850 (WS-C3850-12S-S、WS-C3850-24T)

F5
BIG-IP i2600
BIG-IP LTM 4200
BIG-IP LTM 3900
BIG-IP GTM 1600

Fortinet
FortiGate 3140B
FortiGate 200D
FortiGate 60D
Fortinet 60E

Palo - Alto
PA-3020

CheckPoint
15400

Flow-Base
sFlow
NetFlow version 5 / 7 / 9
ipfix

網路防火牆

OS

Windows/AD Server
Windows Server 2003
Windows Server 2003 R2
Windows Server 2008(Win Server 2008 Standard SP2、Win Server 2008 Enterprise SP2)
Windows Server 2008 R2(Server 2008 R2 Enterprise SP1、Win Server 2008 R2 Standard SP1)
Windows Server 2012Win Server 2012 Standard)
Windows Server 2012 R2(Win Server 2012 R2 Standard)
Windows Server 2016(Win Server 2016 Standard)
Windows Server 2019
Windows 7 Enterprise

Linux
CentOS 7 / 8
Red Hat Enterprise Linux 7 / 8
Ubuntu 18
SUSE Linux Enterprise Server 12 SP 3 / 12 SP4 / 15

Unix
AIX
HP-UX

ESXi
VM Ware ESXi 6.5
VM Ware ESXi 6.0
VM Ware ESXi 5.5

Middleware

DB
Oracle
MS SQL
MariaDB
MySQL
DB2
PostgreSQL
MongoDB
Redis

Container
Docker
Kubernetes

AP
Apache
Nginx
JBoss
Node.js
HAProxy
IIS

功能列表

系統功能

1. 軟體授權不限流量、EPS、容量、CPU、Memory、日誌來源設備數、日誌量及操作使用者數量。
2. 具備高可用性 (HA) 機制，避免單點失效造成日誌查找及其他功能無法正常運作。
3. 具備高擴充性，隨著資料量增加，可透過水平擴充或垂直擴充以維持正常的效能運作，且技術上擴充的節點數無上限。
4. 支援分散式架構，收容之資料會自動備份且分配在各個節點中，並透過分散式架構加速資料查詢。
5. 可透過瀏覽器進行日誌管理及查詢，且支援 SSL 安全加密的 Web 操作介面，包含系統管理設定與使用者操作介面。
6. 支援使用者操作紀錄，如登入及日誌查詢等紀錄。
7. 儀表板 (Dashboard) 支援繁體中文顯示。
8. 可支援雲平台佈建，並支援多租戶服務，提供中控台同時監控多個 SOOP-CLM 叢集使用情況。
9. 可監控本身狀態及各節點狀況，當監控項目有服務異常，會發送告警通知。

資料收集機制

1. 支援收容 Linux、Windows、MSSQL 及 AD Server 日誌資料，且提供相關日誌解析模組進行資料正規化。
2. 若所收容之作業系統或網路設備因版本升級，造成日誌格式更動，內建模組支援更新。
3. 提供代理程式 (Agent) 及無代理程式 (Agentless) 方式收集日誌。
4. 支援多樣日誌蒐集方式，包含 TCP/UDP、SNMP Traps、Syslog、NetFlow、Windows Event Files、CSV、TXT、XML 等。
5. 具備日誌解析緩衝能力，可避免瞬間大量資料湧入而造成資料遺失；並可選購擴充模組將日誌緩衝進階功能建置於獨立伺服器中。
6. 系統支援 IPv6 設備之日誌收集。
7. 日誌儲存採用 NoSQL 運算技術（非傳統 RDBMS），符合大數據資料儲存模式。
8. 可依據不同需求進行客製化日誌解析，且保留日誌資料的原始型內容 (Raw Data) 。
9. 支援 JDBC 連線，可讀取資料庫表格的內容儲存至日誌管理系統。

資料儲存

1. 系統包含資料儲存生命周期管理功能，可依據不同來源設定不同的日誌留存天數，有效精簡硬碟空間的使用；並可選購擴充模組將資料備份至外部儲存空間。

功能列表

資料查詢及呈現

1. 未使用Flash-plugin，以符合資安需求。
2. 支援分散式關聯分析查詢，可由單一查詢條件搜索各分散儲存的日誌與事件並呈現符合之結果。
3. 支援正規表示式 (Regular Expression) 搜尋條件，可查詢任何時間區間、任何設備 (Source)、任何資料型態 (Source Type) 的資訊。
4. 提供圖像化時間軸儀表板 (Timeline Dashboard)，可以於時間軸儀表板上點選特定區間，用以篩選出特定時間點的日誌。
5. 提供多種內建的日誌模板，維運人員僅需將相關日誌資料匯入，即可使用內建之日誌儀表板；如作業系統儀表板 (Windows 及 Linux 等) 提供日誌事件等級趨勢圖表、登入 / 登出事件查詢及關機統計等。防火牆儀表板提供防火牆來源 IP、目的 IP 統計圖表、Deny Policy 相關統計圖表等。

權限控管與資料安全

1. 支援角色 (Role) 權限控管機制，可依照不同角色檢視相對應的資料。
2. 支援群組設定，可針對不同群組設定各群組可查閱的資料內容；如 DB 管理員僅能查閱 DB Audit Log，Windows 管理員僅能查閱 Windows Event Log。
3. 可依據事件內容及關鍵字進行權限設定；如設定相關人員僅能查閱日誌中『同時出現 Event_ID 為 4625(Failed logon) 及 User 為 Administrator』之日誌資料。
4. 具備安全管理機制，避免所收集之日誌與事件紀錄被竄改或刪除。
5. 支援串接 AD/LDAP 及 OIDC。
6. 提供密碼強度設定，支援強制要求密碼需含大小寫英文字母、數字及特殊符號，以配合法規稽核需求。
7. 提供帳號鎖定機制，在帳號登入失敗三次後立即鎖定，以配合法規稽核需求。
8. 儀表板支援權限管控功能，可限定特定的使用者或是角色是否可以閱覽或是修改儀表板。
9. 具備系統自我稽核功能，可即時紀錄與稽核使用者的操作記錄。

報表產出及自動告警

1. 報表內容可包含原始資料表格化或視覺化結果 (如：文字雲、折線圖、長條圖、圓餅圖、散佈圖...等)。
2. 提供報表設定功能，使用者透過介面設定及製作報表。
3. 報表支援 PDF 及 MHTML 格式。
4. 具備報表排程功能，同時支援日報、週報、月報、季報及年報，並可指定報表收件人。
5. 提供自動告警功能，支援關鍵字及條件設定事件告警，並藉由 E-Mail 發送告警給指定人員。
6. 告警郵件內容包含告警狀態及相關事件之日誌內容，如登入失敗告警信件，包含事件發生時間、登入使用的帳號及日誌內文。
7. 告警功能支援動態閾值，根據先前的行為模式，辨識系統中異常的事件，提供真實動態趨勢分析，避免僅靠靜態閾值判定造成的誤差。

EPS 2,300 情境舉例

EPS 2,300 日誌資料，單次查詢區間 1 day，SOOP-CLM 保留 20 天的資料

產品名稱

SOOP-CLM 企業版 (HA 版本，且資料備份 1 份)

3台硬體資源

CPU: 16 Core

Memory: 256 GB

Disk: IOPS 500+, 3.5 TB

支援OS版本

RHEL

8.8 x64 Minimal

Ubuntu

Ubuntu Server 22.04

此規格可收容資料

1. 單筆日誌大小 1 KB。
2. EPS 2,300 日誌資料。
3. 5 種不同來源類型的日誌資料 (如 Windows、Cisco、F5 都各自算一類)。
4. 單次查詢區間 1 day，並於 SOOP-CLM 保留 20 天的資料。

CLM各版本功能比較表

系統功能	旗艦版	企業版	標準版
1 軟體授權不得限制，授權不限流量、EPS、容量、CPU、Memory、日誌來源設備數、日誌量及操作使用者數量	✓	✓	✓
2 系統架構需具備 HA 機制，避免單點失效造成日誌查找及其他功能無法正常運作	✓	✓	✗
3 系統架構須具備高擴充性，隨著資料量增加，可透過水平擴充或垂直擴充以維持正常的效能運作，且技術上擴充的節點數無上限	✓	✓	✓
4 支援分散式架構，收容之資料會自動備份且分配在各個節點中，並透過分散式架構加速資料查詢	✓	✓	✗
5 可透過瀏覽器進行日誌管理及查詢，且須支援 SSL 安全加密的 Web 操作介面，包含系統管理設定與使用者操作介面	✓	✓	✓
6 系統需提供使用者操作紀錄，如登入及日誌查詢等紀錄	✓	✓	✓
7 儀表板 (Dashboard) 支援繁體中文顯示	✓	✓	✓
8 可建置於雲環境	✓	✗	✗
9 支援多租戶服務	✓	✗	✗
10 可監控本身狀態及各節點狀況	✓	✓	✓
11 自我監控可自定義需要之告警門檻值，如 Disk 告警門檻值	✓	✗	✗
12 當監控項目有服務異常，除了會發送告警通知，SOOP-CLM 服務也會先自動重啟，以維持系統高穩定度	✓	✗	✗

CLM各版本功能比較表

系統功能	旗艦版	企業版	標準版
13 節點設定資料互相備援，當主節點失效時，會自動由另一個節點接續主節點的所有工作，如告警、排程報表、資料分配等	✓	✗	✗
14 支援 SOOP-CLM Plus - Archive 單一登入窗口	✓	✗	✗
15 支援 SOOP-CLM Plus - Data Queue Cluster 單一登入窗口	✓	✗	✗
16 具備設備差異比較相關儀表板，以視覺化方式列出新增的設備或被移除的設備，有效進行納管設備管理	✓	✗	✗
17 支援 ETL(extract, transform and load) 功能，可將兩筆不同之日誌進行運算，如計算兩筆 log 的時間差	✓	✗	✗
18 支援單一節點重建機制，以因應硬體故障時，需替換硬體之需求	✓	✗	✗
19 支援重要設定檔匯入匯出機制，以因應系統異常或任何操作問題，需將設定重新倒回之情境	✓	✗	✗
20 支援機敏資料保護機制，遮罩如身分證字號或電話號碼的機敏訊息	✓	✗	✗
21 內建 GeoIP 資料庫，可將日誌中的 IP 資訊轉換為經緯度資訊	✓	✗	✗
22 可透過地圖方式呈現經緯度資訊，如於地圖畫面呈現各地日誌數量或異常情況	✓	✗	✗
23 提供 API User 機制，供第三方軟體介接，取得日誌資料進行應用	✓	✗	✗

CLM各版本功能比較表

	權限管控	旗艦版	企業版	標準版
1	有效控管使用者日誌查詢權限，透過Role-based access control 有效保護日誌資料	✓	✓	✓
2	內建Document Level Security，能依內容細分權限等級	✓	✗	✗
3	支援AD/LDAP及OIDC帳號串接	✓	✓	✓
4	可設定密碼複雜度、登入錯誤鎖密碼機制	✓	✓	✓
5	符合ISO 27001與PCI DSS等日誌合規/稽核規範	✓	✓	✓
6	支援AD群組同步功能	✓	✗	✗
7	可設定特定帳號只能進入前台進行資料查找，禁止登入後台進行告警或模組等管理設定	✓	✗	✗
	資料留存			
1	依據不同來源設定不同的日誌留存天數，有效精簡硬碟空間的使用；並可將資料備份給外部儲存空間	✓	✓	✓
	資料收集及查詢機制			
1	提供大量隨插即用的日誌解析模板，維運人員僅需將相關日誌資料匯入，內建之高可讀性儀表板立即呈現	✓	△	△
2	內建OS模組：ESXi、Windows、AD Server、CentOS、Red Hat Enterprise Linux、Ubuntu、SUSE Linux Enterprise Server、Unix、AIX、HP-UX	✓	✓	✓

PiExtract 信研科技股份有限公司
MAIL : support@piextract.com

CLM各版本功能比較表

資料收集及查詢機制	旗艦版	企業版	標準版
3 內建網路設備模組：Flow-Base、F5、Cisco、NetFlow、sFlow	✓	✓	✓
4 內建防火牆模組：Fortinet、Checkpoint、Palo-Alto	✓	✓	✓
5 內建Middleware模組：Apache、Nginx、JBoss、Node.js、HAProxy、IIS	✓	✓	✓
6 內建DB模組：Oracle、MS SQL、MariaDB、MySQL、DB2、PostgreSQL、MongoDB、Redis	✓	✓	✓
7 內建Container模組：Docker、Kubernetes	✓	✓	✓
8 內建OS模組：IBM AS/400	✓	✗	✗
9 內建網路設備模組：Aruba、A10、Ixia、Juniper	✓	✗	✗
10 內建Middleware模組：CyberArk、Infoblox、Imperva	✓	✗	✗
11 內建端點防護軟體模組：Symantec、Netapp Storage	✓	✗	✗
12 提供代理程式(Agent)及無代理程式(Agentless)方式收集日誌，如Disk告警門檻值	✓	✗	✗
13 支援多樣日誌蒐集方式，包含 TCP/UDP、SNMP Traps、Syslog、NetFlow、Windows Event Files、CSV、TXT、XML等	✓	✓	✓
14 具備日誌解析緩衝能力，可避免瞬間大量資料湧入而造成資料遺失。	✓	✓	✓
15 系統支援IPv6設備之日誌收集	✓	✓	✓

CLM各版本功能比較表

資料收集及查詢機制

		旗艦版	企業版	標準版
16	採用NoSQL運算技術(非傳統RDBMS)，符合大數據資料儲存模式	✓	✓	✓
17	支援JDBC連線，可讀取資料庫表格的內容儲存至日誌管理系統。	✓	✓	✓
18	支援分散式關聯分析查詢，可由單一查詢條件搜索各分散儲存的日誌與事件並呈現符合之結果	✓	✓	✓
19	支援正規表示式(Regular Expression)搜尋條件，可查詢任何時間區間、任何設備(source)、任何資料型態(source type)的資訊	✓	✓	✓
20	提供資料整理與運算功能，例如字串處理、欄位動態增刪等	✓	△	△
21	提供圖像化時間軸儀表板(timeline dashboard)，可以於時間軸儀表板上點選特定區間，用以篩選出特定時間點的日誌	✓	✓	✓
22	提供客製化解析介面，讓使用者可以自行開發新的日誌解析功能	✓	✗	✗
23	支援第三方監控工具收集效能數據，滿足客戶擴充監控需求	✓	✗	✗
24	透過日誌欄位命名規則，自動對應該欄位之資料類型，以避免資料欄位衝突，如欄位名稱為_date結尾之欄位，會自動判定資料類型為日期，並進行對應之資料處理。	✓	✗	✗
25	日誌解析設定，可透過單一頁面，指定特定解析規則只針對特定節點生效，以達到資源規劃分配使用之用途。	✓	✗	✗
26	提供日誌template設定功能，使用者可透過此功能設定個資料來源的資料欄位及對應之資料類型。	✓	✗	✗

CLM各版本功能比較表

告警設定

		旗艦版	企業版	標準版
1	提供自動告警功能，支援關鍵字及條件設定事件告警，並藉由E-Mail發送告警給指定人員	✓	✓	✓
2	支援整合其他告警平台，如Email, SMS, 常見通訊軟體	✓	✗	✗
3	告警郵件內容須包含告警狀態及相關事件之日誌內容，如登入失敗告警信件，包含事件發生時間、登入使用的帳號及日誌內文	✓	✓	✓
4	告警功能支援動態閾值，根據先前的行為模式，辨識系統中異常的事件，提供真實動態趨勢分析，避免僅靠靜態閾值判定造成的誤差	✓	✗	✗
5	告警事件支援failed shard狀態，可有效避免效能不足時，造成大量告警勿報的情況發生	✓	✗	✗

報表功能

1	提供報表設定功能，使用者透過介面設定及製作報表，支援PDF及HTML格式	✓	✓	✓
2	PDF報表可自定logo，可透過此功能將客戶logo附錄至PDF報表中進行寄送	✓	✗	✗
3	可將查詢結果之原始資料(raw data)匯出爲CSV	✓	✓	✓
4	報表內容能包含原始資料表格化或視覺化結果(如：文字雲、折線圖、長條圖、圓餅圖、散佈圖...等)	✓	✓	✓
5	定期將 Dashboard 匯出為 PDF格式，並寄送至使用者信箱；定期提供管理人員系統維運報告	✓	✓	✓
6	排程報表支援filter機制，可透過此機制對報表統計的資料進一步進行過濾，如同一張windows的報表，可設定不同之filter，發送給不同的管理人員	✓	✗	✗

PiExtract 信研科技股份有限公司
MAIL : support@piextract.com