TAICS

TAICS TR-0033 v1.0:2024

5G虛擬化網路資安指引 -Kubernetes安全設定

Cybersecurity Guidelines for 5G virtualisation network - Security configuration for Kubernetes

2024/10/28

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

5G 虛擬化網路資安指引-Kubernetes 安全設定

Cybersecurity Guidelines for 5G virtualisation network – Security configuration for Kubernetes

出版日期: 2024/10/28
終審日期: 2024/09/26

誌謝

本指引由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC5 主席：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人工業技術研究院 黃維中 副所長

TC5 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC5 副主席：財團法人電信技術中心 林炫佑 副執行長

TC5 行動通訊資安工作組組長：財團法人資訊工業策進會 柯盈圳 組長

技術編輯：財團法人資訊工業策進會 劉恩賜 資深研發經理、蔡宜學 資深技術經理

此指引制定之協會會員參與名單為(以中文名稱順序排列)：

中華資安國際股份有限公司、中華電信股份有限公司、台達電子工業股份有限公司、台灣大哥大股份有限公司、台灣檢驗科技股份有限公司、和碩聯合科技股份有限公司、英業達股份有限公司、神盾股份有限公司、財團法人工業技術研究院、財團法人資訊工業策進會、國立陽明交通大學、國立臺北大學、華電聯網股份有限公司、華碩電腦股份有限公司、雲達科技股份有限公司、遠傳電信股份有限公司、德凱認證股份有限公司、緯創資通股份有限公司、趨勢科技股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

國立雲林科技大學

本指引由數位發展部支持研究制定。

目錄

前言

本指引係依台灣資通產業標準協會(TAICS)之規定，經技術管理委員會審定，由協會公布之產業指引。

本指引並未建議所有安全事項，使用本指引前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本指引之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

全球電信事業深刻感受到需要透過新的 Open RAN 的網路標準規範，達成更具競爭性與動態彈性的無線接取網路(Radio Access Network, RAN)供應鏈，積極推動 Open RAN 的網路架構以打破過去軟硬體高度整合的常態。在 Open RAN 標準化與開放過程中，需要透過眾多產業間的合作與溝通，以便在全球推動無線開放網路、軟體和虛擬化的目標。隨著 5G 行動通訊網路標榜以服務基礎架構(Service-Based Architecture, SBA)為導向之網路功能虛擬化(Network Function Virtualisation, NFV)為基礎架構解決方案後，開放式架構 Open RAN 也大多採用 Kubernetes (K8s)網路功能虛擬化(NFV)為基礎架構解決方案後，市場也擔心網路功能虛擬化架構會不會讓資安漏洞更多。

為了解決 5G 網路功能虛擬化架構的資安議題，第三代合作夥伴計畫(The 3rd Generation Partnership Project, 3GPP)的安全性工作群組(SA3 Security)於 2018 年新增第三代合作夥伴計畫虛擬化產品安全保證方法與資安確保標準(Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products)研究項目。且開放式無線接取網路聯盟(O-RAN Alliance)於 2022 年正式成為第十一工作小組(Working Group 11, WG11)之安全工作小組(Security Working Group, SWG)，專注於制定 Open RAN 網路產品的安全架構和安全保證規範，訂定開放式無線接取網路安全架構與框架，推動產品資安保證評估驗證程序。

有鑑於 5G 多元應用型態於國內佈建獨立組網(Standalone, SA)系統架構時需要依賴 5G Open RAN 基地臺，在數位發展部數位產業署「5G 資安防護系統開發計畫」的支持下，資策會資安所團隊參考國際標準作法第三代合作夥伴計畫的安全性工作群組及無線接取網路聯盟的安全工作小組訂定之 5G 系統通訊產品資安確保標準，制定相關的資安測試細節，並於台灣資通產業標準協會進行產業標準制定，以凝聚相關產、官、學、研各界共識。

「TAICS TR-0033 5G 虛擬化網路資安指引-Kubernetes 安全設定」(以下簡稱本指引)，參考 TAICS TR-0017 v1.0「5G 專網多接取邊緣運算資安研究報告」及 TAICS TR-0025 v1.0「5G Open RAN 資安研究報告」與第三代合作夥伴計畫(3GPP)之標準規範的

資安測試指引細節。本指引建議資安要求指引等事項，俾利 5G 通訊設備製造商、系統整合商及 5G 資安檢測實驗室等作為相關產品設定安全的參考指引。

1. 適用範圍

本指引定義 Kubernetes (K8s) 容器架構之安全設定要求，此為 5G 獨立組網 (Standalone, SA) 網路功能虛擬化基礎建設 (Network Functions Virtualisation Infrastructure, NFVI) 虛擬層 (virtualisation layer)之容器管理協作平台架構。該系統架構引用第三代合作夥伴計畫 3GPP 33.927 相關定義之架構，如下圖 1 所示。本指引適用範圍包括支援下圖紅框標註部分採用 Kubernetes 容器架構的虛擬化網路層，但採用其它架構的虛擬化網路層不在本指引規範之範圍。本指引適用對象為採用 Kubernetes 容器架構的 5G 通訊設備製造商、系統整合商及檢測該架構的 5G 資安檢測實驗室等，以強化 Kubernetes 容器管理協作平台架構之安全性。

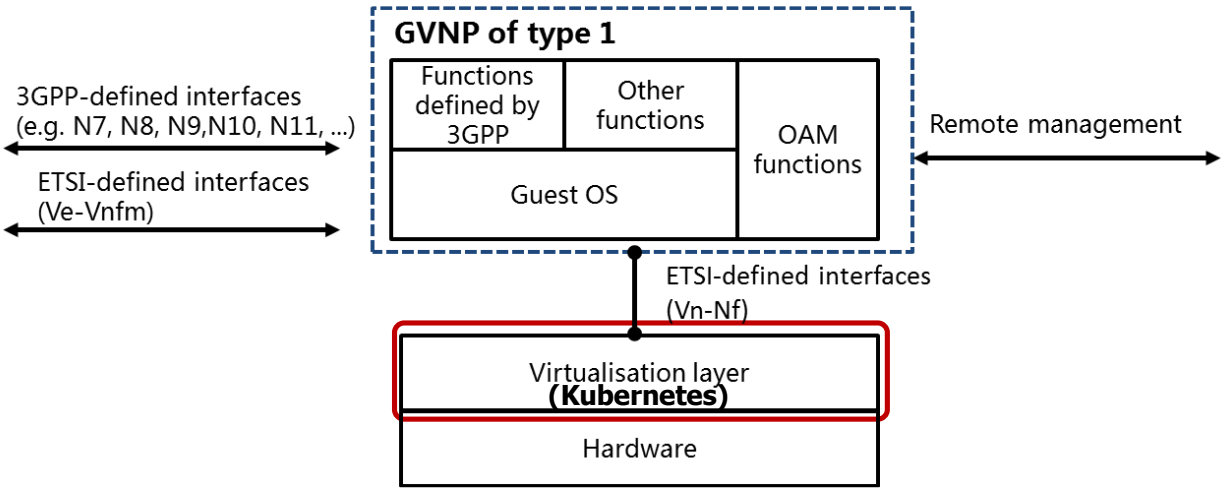

圖 1 適用範圍示意圖

2. 引用標準

下列法規、標準或文件因本指引所引用，引用章節之內容成為本指引之一部分。有加註年份者，適用該年份之版次，不適用於其後之修訂版(含補充增修)。無加註年份者，適用其最新版(含補充增修)。

[1] TAICS TR-0017 v1.0:2021, “5G 專網多接取邊緣運算資安研究報告”

[2] TAICS TR-0025 v1.0:2022, “5G Open RAN 資安研究報告”

[3] 3GPP TR 33.818-h10, “Security Assurance Methodology (SECAM); and Security Assurance Specification (SCAS)for 3GPP virtualised network products (Release 17)”

[4] 3GPP TR 33.936-i01, “Security Assurance Methodology (SECAM) for 3GPP virtualized network products”

[5] 3GPP TR 33.927-i01, “threats and critical assets in 3GPP virtualized network product classes”

[6] O-RAN.WG11.SecTestSpecs，”O-RAN Security Test Specifications fromO-RAN Work Group 11 (Security Work Group)”

3. 用語及定義

下列用語與定義適用於本指引。

3.1 第三代合作夥伴計畫 (The 3rd Generation Partnership Project, 3GPP)

是一個成立於 1998 年 12 月的標準化機構，該機構設立的原初目的在推廣以全球行動通訊系統 (Global System for Mobile communications, GSM) 規格為基礎的國際行動通訊 2000 (International Mobile Telecommunication-2000, IMT-2000) 技術規範，提出一個能持續演進強化的國際通用技術標準規格，並於 2018 年 6 月與 2020 年 7 月正式完成 5G 獨立組網 (Standalone, SA) 第 15 版本 (Release 15) 以及第 16 版本 (Release 16) 的標準制定。目前其成員包括歐洲電信標準化協會 (European Telecommunications Standards Institute, ETSI)、日本無線電產業與商務協會 (Association of Radio Industries and Business, ARIB)、日本電信技術委員會 (Telecommunication Technology Committee, TTC)、中國通訊標準化協會 (China Communications Standards Association, CCSA)、北美通訊產業解決方案聯盟 (Alliance for Telecommunications Industry Solutions, ATIS)、韓國電信技術協會 (Telecommunication Technical Assembly, TTA)，以及印度電信標準發展協會 (Telecommunications Standards Development Society, India, TSDSI) 都簽署加入這個合作性協議中。

3.2 開放式無線接取網路聯盟 (Open Radio Access Network Alliance, O-RAN Alliance)

是一個成立於 2018 年 2 月的標準化機構，該機構由雲端無線接取網路聯盟(Cloud Radio Access Network Alliance, C-RAN Alliance)與 xRAN 論壇(xRAN Forum)兩個組織合併組成，以推動在全球無線網路方面的開放網路、軟體和虛擬化目標。在 Open RAN 標準化與開放過程中，需要透過眾多產業間的合作與溝通，以便在全球推動無線開放網路、軟體和虛擬化的目標。如透過開放性無線接取網路政策聯盟(Open RAN Policy Coalition)、開放測試與整合中心(Open Test and Integration Center, OTIC)、電信基礎架構專案(Telecom Infra Project, TIP)與開放網路基金會(Open Networking Foundation, ONF)和

Linux 基金會(Linux Foundation)以及全球行動通訊系統協會(Groupe Speciale Mobile Association, GSMA)等不同層面的單位各自投入發展開放式軟硬體的架構。

3.3 安全保證規範(Security Assurance Specification, SCAS)

涵蓋 O-CU、gNB 及 5GC 的七大資安威脅面向與相關資安測試案例，針對生產製造的行動通訊裝置進行合規檢測，並由資安實驗室針對設備的弱點進行規範檢測及防駭漏洞檢測等兩階段資安檢測。

3.4 網路設備安全保證方案 (Network Equipment Security Assurance Scheme, NESAS)

包含了設備供應製造商的開發與產品生命週期之驗證、測試實驗室之認證、網路設備之安全性測試評估規範，針對支援第三代合作夥伴計畫(The 3rd Generation Partnership Project, 3GPP)定義功能網路產品的供應商構建安全認證框架，以提升行動產業的安全層級。並由全球行動通訊系統協會(Groupe Speciale Mobile Association, GSMA)負責管理、制定並定期修訂規範內容。

3.5 商用現成軟體 (Commercial-off-the-shelf, COTS)

是指事先寫好的一組應用程式軟體，並在市場上販售交易，讓個人或企業組織不需要再為特定的功能撰寫自己的軟體程式。

3.6 自由及開放原始碼軟體 (Free-open-source-software, FOSS)

是自由軟體與開源軟體的總稱。與專有軟體(proprietary software)相對，其原始碼通常為公開共享，在授權下可供所有人免費使用、修改和分發，鼓勵人們志願改善軟體設計。使用 FOSS 的好處包括降低軟體成本、提高對惡意軟體的安全性、穩定性、隱私性，以及讓使用者對自己的硬體有更多掌控能力。

3.7 Kubernetes (K8s) 容器架構

一套由 Google 設計出來用於自動化部署、擴展與管理容器化應用程式的開源系統，它支援了多種不同的容器工具如 Docker 等。

4. 分析 5G 資安風險與需求

依據 3GPP TR 33.927 與 3GPP TR 33.926 定義網路產品類別之威脅和關鍵資產的安全保證規範(Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes)，從 5G 資安風險分析可以歸納出八種威脅層面的主要威脅，分別為 3GPP 定義的網路介面威脅(Threats Relating to 3GPP-defined Interfaces)、ETSI 定義的網路介面威脅(Threats Relating to ETSI-defined Interfaces)、身分識別欺騙(Spoofing Identity)、竄改(Tampering)、否認性(Repudiation)、資訊揭露(Information Disclosure)、阻斷服務(Denial of service)以及特權提升(Elevation of Privilege)，其中針對 5G 虛擬化網路風險分析如表 1 所示。

表 1 5G 虛擬化網路風險評估

威脅種類	威脅項目	威脅細節
3GPP 定義的網路介面威脅(Threats relating to 3GPP-defined interfaces)	N2 介面威脅	資料竄改、資料洩漏、服務阻斷
	N3 介面威脅	資料竄改、資料洩漏
	Xn 介面威脅	資料竄改、資料洩漏
	NR-Uu 介面威脅	資料竄改、資料洩漏
身分識別欺騙 (Spoofing identity)	預設帳戶 (Default Accounts)	使用預設之弱密碼非法登入
	弱密碼政策(Weak Password Policies)	暴力破解弱密碼非法登入
	窺視密碼 (Password peek)	明文密碼記錄於他人可視之處，而以該密碼非法登入
	直接根存取 (Direct Root Access)	可直接存取 root 帳號，以暴力破解登入
	網際通訊協定欺騙 (IP Spoofing)	將封包的原始 IP 改成偽冒的合法來源 IP，傳送至受害主機
	惡意程式 (Malware)	阻斷服務、資訊外洩、提權
	竊聽 (Eavesdropping)	資訊外洩
竄改 (Tampering)	軟體竄改 (Software Tampering)	阻斷服務、資訊外洩、提權
	所有權檔案誤用(Ownership File Misuse)	阻斷服務、資訊外洩
	開機竄改 (Boot tampering)	阻斷服務、資訊外洩、提權
	日誌竄改 (Log Tampering)	事件調查與鑑識難度增加
	營運管理與維護流量竄改 (OAM traffic Tampering)	阻斷服務、資訊外洩
	檔案寫入權限濫用 (File Write Permissions Abuse)	阻斷服務、資訊外洩、提權

	用戶通信期竄改 (User Session Tampering)	非法登入
否認性 (Repudiation)	缺乏用戶活動記錄 (Lack of User Activity Trace)	事件調查與鑑識難度增加
資訊揭露 (Information disclosure)	不良金鑰產生 (Poor key generation)	加密傳輸遭破解
	不良金鑰管理 (Poor key management)	加密傳輸遭破解
	弱密碼演算法 (Weak cryptographic algorithms)	加密傳輸遭破解
	不安全資料儲存 (Insecure Data Storage)	機敏資料外洩
	系統指紋 (System Fingerprinting)	駭客情搜攻擊目標之相關資訊，作為進階攻擊之前置作業
	惡意程式 (Malware)	阻斷服務、資訊外洩、提權
	個人識別資訊違規 (Personal Identification Information Violation)*	個人資料外洩
	不安全預設組態 (Insecure Default Configuration)	阻斷服務、資訊外洩、提權
	檔案/目錄讀出權限濫用 (File/Directory Read Permissions Misuse)	阻斷服務、資訊外洩、提權
	不安全網路服務 (Insecure Network Services)	阻斷服務、資訊外洩、提權
	非必要服務 (Unnecessary Services)	阻斷服務、資訊外洩、提權
	日誌揭露 (Log Disclosure)	資訊外洩
	非必要應用 (Unnecessary Applications)	資訊外洩
	竊聽 (Eavesdropping)	傳輸資料外洩
	缺乏通用網路產品流量隔離導致安全威脅 (Security threat caused by lack of GNP traffic isolation)	傳輸資料外洩、資料非法存取
阻斷服務 (Denial of Service)	被破解/行為異常用戶設備 (Compromised/Misbehaving User Equipment)*	產生異常連線來阻斷服務
	實作缺陷 (Implementation Flaw)*	阻斷服務、資訊外洩、提權
	不安全網路服務 (Insecure Network Services)	阻斷服務、資訊外洩、提權
	人為錯誤 (Human Error)*	阻斷服務、資訊外洩、提權
特權提升 (Elevation of privilege)	授權使用者誤用 (Misuse by authorized users)*	使用者權限設置不當、未監管最高管理者權限之行為
	超過特權的程序/服務 Over-Privileged Processes/Services	以特權程序執行惡意程式碼
	資料夾寫入權限濫用 (Folder Write Permission Abuse)	寫入惡意程式檔案
	根所屬檔案寫入權限濫用 (Root-	以 Root 執行惡意程式

	Owned File Write Permission Abuse)	
	高特權檔案 (High-Privileged Files)	一般使用者非法執行高特權檔案
	不安全網路服務 (Insecure Network Services)	阻斷服務、資訊外洩、提權
	透過非必要網路服務特權提升 (Elevation of Privilege via Unnecessary Network Services)	阻斷服務、資訊外洩、提權

註* 需要透過營運機構之通信系統資通安全維護的「管理面」與「制度面」來避免本威脅

5. 資安要求指引分類

本指引參考 TAICS TR-0017 v1.0「5G 專網多接取邊緣運算資安研究報告」及 TAICS TR-0025 v1.0「5G Open RAN 資安研究報告」與第三代合作夥伴計畫(3GPP)之標準規範，針對訂定資安要求指引之實施細節。根據 5G ORAN 可能遭遇威脅並且針對 Kubernetes 安全特性來擬定相關資訊安全要求指引，如表 2 所示

表 2 Kubernetes 安全設定檢測項目總表

資安指引章節	分類	資安要求項目
6.1.1	身分識別欺騙(Spoofing identity)	SI01 使用安全認證方式
6.1.2	身分識別欺騙(Spoofing identity)	SI02 避免啟動匿名存取功能
6.1.3	身分識別欺騙(Spoofing identity)	SI03 Secret 等機敏資料應預設加密
6.1.4	身分識別欺騙(Spoofing identity)	SI04 避免允許所有 API 請求
6.1.5	身分識別欺騙(Spoofing identity)	SI05 應確認容器(container)使用 image 之安全性
6.1.6	身分識別欺騙(Spoofing identity)	SI06 Etcd 連線應加密
6.2.1	竄改(Tampering)	TA01 檢視系統軟體版本已知漏洞
6.2.2	竄改(Tampering)	TA02 檔案擁有者權限安全
6.2.3	竄改(Tampering)	TA03 開機僅可透過合法的韌體
6.2.4	竄改(Tampering)	TA04 應使用加密協定進行連線
6.2.5	竄改(Tampering)	TA05 重要設定檔案權限管控
6.2.6	竄改(Tampering)	TA06 確保應用程式 session 隨機安全性
6.3.1	否認性(Repudiation)	RE01 應有使用者行為之軌跡與紀錄
6.4.1	資訊揭露(Information disclosure)	ID01 應使用安全金鑰長度
6.4.2	資訊揭露(Information disclosure)	ID02 應強化設定金鑰管理存取權限
6.4.3	資訊揭露(Information disclosure)	ID03 應使用安全金鑰演算法
6.4.4	資訊揭露(Information disclosure)	ID04 應避免預設不安全設定
6.4.5	資訊揭露(Information disclosure)	ID05 應妥善設定重要檔案與資料夾存取權限
6.4.6	資訊揭露(Information disclosure)	ID06 開啟最小化需求之網路服務
6.4.7	資訊揭露(Information disclosure)	ID07 稽核紀錄保存管理
6.5.1	阻斷服務(Denial of Service)	DS01 應限制來自外部之異常連線或阻斷服務攻擊
6.6.1	提高特權(Elevation of privilege)	EP01 避免共用預設 namespace
6.6.2	提高特權(Elevation of privilege)	EP02 避免最高權限遭非法濫用

6. 資安要求指引

6.1 身分識別欺騙(Spoofing identity)

6.1.1 SI01 使用安全認證方式

6.1.1.1 指引說明

避免使用不安全認證機制(如 token 認證)，若使用固定 bearer tokens 與 API server 進行認證，API server 將讀取 bearer tokens 檔案，且 bearer tokens 無有效期限，及 bearer tokens 於未重開 API server 情況下是無法被改變。因其固定 Token 為明文儲存之檔案，若外洩或遭非法存取，可能遭偽冒認證；且因 Token 無有效期限，故無法定期系統要求更改，可能有遭破解之風險。

授權模式(authorization mode)將針對已認證之 API 請求進行授權審核之機制，應依需求妥善設定管理，避免設定 AlwaysAllow，此設定為 API server 允許所有的 API 請求，可能有遭未授權之連線存取系統之風險。建議至少設定為 Node 或 Role-based access control (RBAC)，以安全管理來自外部的 API 請求。

6.1.1.2 安全要求

(a) 參數 token-auth-file 應不得設定

(b) 參數 authorization-mode 應不得設定為 AlwaysAllow

(c) 參數 authorization-mode 參數應包含 Node、RBAC

6.1.2 SI02 避免啟動匿名存取功能

若啟動匿名存取功能，API server 可接受「匿名請求」之連線，且該匿名請求將不再受到認證機制的要求，並給予使用者為 system:anonymous 與群組為 system:unauthenticated。建議避免啟動匿名存取功能，若允許匿名登入，請求將不用受到認證限制，非法使用者可以送出相關惡意請求，可能有非法存取風險。

6.1.2.1 安全要求

(a) anonymous-auth 參數應不得設定為 true

6.1.3 SI03 Secret 等機敏資料應預設加密

6.1.3.1 指引說明

Secret 為 kubernetes 的一個重要元件，主要為使用於儲存 Pod 或容器所使用之機敏資料，可能包含個人資料、帳號密碼、Tokens、信用卡資料、金鑰等，並儲存於 API server。預設情況下，Secret 為未加密儲存於 API server 的 etcd，任何擁有 API server 連線權限的使用者皆可讀取或修改 Secret，此外，命名空間(namespace)中擁有創建 Pod 權限的使用者皆可以存取該命名空間中的任何 Secret。因 Secret 含有相關機敏資料，建議應啟用加密機制來保護 Secret 等機敏資料，並依需求妥善設定 encryption-provider-config，倘若外洩可能有直接暴露之風險時，應不以明文儲存機敏資料。

6.1.3.2 安全要求

(a) API server 應啟用參數 encryption-provider-config，並依需求妥善設定

6.1.4 SI04 避免允許所有 API 請求

建議 API server 避免允許所有之 API 請求，若允許所有 API 請求，可能有非法存取之風險。應根據需求設定准入控制器(enable admission plugins)，檢視其設定未包含 AlwaysAdmit，因此設定將允許所有 API 請求，可能存在非法存取之風險。

6.1.4.1 安全要求

(a) 參數 enable-admission-plugins 應不得設定 AlwaysAdmit

6.1.5 SI05 應確認容器(container)使用 image 之安全性

6.1.5.1 指引說明

建議確認容器(container)相關管控安全性，包含 disable admission plugins 為設定停用的管控元件，其設定應不得包含 ServiceAccount 與 NamespaceLifecycle；enable admission plugins 為啟用的管控元件，其設定應包含 NodeRestriction。

Insecure bind address 設定為允許任何人透過不安全的網路埠連線至主要節點(master node)而不用通過認證與授權，應不得設定此參數。

Secure port 設定為指定特定網路埠連線使用 HTTPS 加密協定，建議未停用此設定。

6.1.5.2 安全要求

(a) disable-admission-plugins 參數的設定值應不得包含 ServiceAccount

(b) disable-admission-plugins 參數的設定值應不得包含 NamespaceLifecycle

(c) enable-admission-plugins 參數設定應包含 NodeRestriction

(d) insecure-bind-address 參數應尚未設置

(e) secure-port 參數應尚未設置為 0

6.1.6 SI06 Etcd 連線應加密

6.1.6.1 指引說明

Etcd 連線應加密，因 Etcd 與客戶端之連線未加密，可能有遭中間人監聽竊取機敏資料之風險，建議以 TLS 加密保護 Etcd 與客戶端之連線，API server 之 etcd certfile 與 etcd keyfile 參數建議設定合適之憑證，並且啟用 service account lookup 參數來驗證 token 是否正確，及設定 service account key file 參數設定憑證檔案來進行驗證。

6.1.6.2 安全要求

(a) service-account-lookup 應已啟用

(b) service-account-key-file 應設定相關金鑰檔案

(c) API server 之--etcd-certfile 與 --etcd-keyfile 參數應已設定合適之憑證

6.2 竄改 (Tampering)

6.2.1 TA01 檢視系統軟體版本已知漏洞

應定期檢視系統軟體版本已知漏洞，包含 Kubernetes 軟體、作業系統、Kubernetes 安裝相關軟體元件及以容器(container) images 所產生 pod，皆可能存在攻擊脆弱點，或者不當存取、修改及刪除機敏資料，皆可能造成系統相關風險。建議應定期檢視作業系統、Kubernetes 軟體、Kubernetes 安裝相關軟體元件及容器(container) images 版本與其對應漏洞資訊，並進行安全掃描、風險評估、弱點識別及修復已知漏洞或防範潛在威脅。

6.2.2 TA02 檔案擁有者權限安全

6.2.2.1 指引說明

確認重要設定檔案權限安全，管控檔案避免遭非擁有者惡意使用，確認 Kubernetes 之 admin.conf、scheduler、controller-manager 重要設定的檔案擁有者權限設定為最高管理者權限，若未妥善控管權限，可能有遭非法存取之風險。

6.2.2.2 安全要求

建議以下檔案應設定僅有 root 可存取

(a) /etc/kubernetes/admin.conf

(b) /etc/kubernetes/scheduler.conf

(c) /etc/kubernetes/controller-manager.conf

6.2.3 TA03 開機僅可透過合法的韌體

應使用合法韌體開機，避免非法韌體藏有後門程式或惡意軟體，影響系統安全。建議檢視 kubernetes 系統設備開機時指定的韌體是否為官方或可信用之來源，以確認開機韌體與系統之安全性。

6.2.4 TA04 應使用加密協定進行連線

6.2.4.1 指引說明

Kubernetes API 為 Kubernetes 控制層之核心元件，而 Kubelet 為 Kubernetes 的每個節點上運行的主要代理元件，用途為跟 Kubernetes API server 註冊、連線、認證及傳遞指令資料等，故從 API server 到 Kubelets 的連線可能傳輸機敏資料，例如 secrets 和金鑰。因此，在 API server 到 Kubelets 之間建議使用加密連線(啟用 kubelet-https)來防護連線安全。若連線未加密，傳輸機敏資料可能遭中間監聽竊取之風險。

預設情況下，API server 不會對 Kubelets 的 HTTPS 端點與匿名請求處理進行身份驗證。建議設置 Kubelet 憑證來進行身份驗證，設定啟用 kubelet-client-certificate 憑證檔案與 kubelet-client-key 金鑰檔案，以確保 API server 與 Kubelets 連線為受到身分驗證保護。

API server 為 Kubernetes 主要節點重要元件，其傳輸包含機敏資料，建議 API server 應該啟用 TLS 加密協定，以 HTTPS 進行傳輸資料，以保護連線安全。設定取用 API server 之 tls-cert-file 憑證與 tls-private-key-file 私鑰。

6.2.4.2 安全要求

(a) 應啟用--kubelet-https

(b) 應設定系統 kubelet-client-certificate 與 --kubelet-client-key 參數

(c) 應設定系統 tls-client-certificate 與 --tls-client-key 參數

6.2.5 TA05 重要設定檔案權限管控

6.2.5.1 指引說明

重要設定檔案應加以管控以避免遭非法存取、竄改與刪除，且 etcd、scheduler、controller-manager、API server pod 等檔案權限建議採最小化設定。未妥善控管權限，則系統存在遭非法存取與異常之風險。

6.2.5.2 安全要求

(a) kube-scheduler.yaml 檔案權限應設定「擁有者能讀取與寫入、群組者能讀取、其他能讀取」，或更嚴格

(b) etcd data 資料夾檔案權限應設定「擁有者能讀取與寫入及執行、群組者無權限、其他無權限」，或更嚴格

(c) admin.conf 檔案權限應設定「擁有者能讀取與寫入、群組者能讀取、其他能讀取」，或更嚴格

(d) scheduler.conf 檔案權限應設定「擁有者能讀取與寫入、群組者能讀取、其他能讀取」，或更嚴格

(e) controller-manager.conf 檔案權限應設定「擁有者能讀取與寫入、群組者能讀取、其他能讀取」，或更嚴格

6.2.6 TA06 確保應用程式 session 隨機安全性

6.2.6.1 指引說明

Kubernetes 可用來建置網站服務，建議網站服務應有身分驗證與授權管理機制，並以 session 管控連線。若有網站服務對外服務，建議確認 session 為唯一不可重複、無特定規律隨機產生及未包含以明文顯示的機敏資訊(例如帳號或個資等)。

6.2.6.2 安全要求

(a) session 應為唯一不可重複

(b) session 產生應該隨機且無特定規律

(c) session 不應包含以明文顯示的敏感資訊(例如帳號等)

6.3 否認性 (Repudiation)

6.3.1 RE01 應有使用者行為之軌跡與紀錄

6.3.1.1 指引說明

Kubernetes API Server 提供了一種安全相關的稽核記錄機制，記錄包含各個用戶、管理者、系統元件及具有影響系統之活動紀錄。Kubernetes 預設僅提供基本的稽核記錄功能，建議可以通過設置適當的稽核記錄日誌路徑(audit-log-path 參數)來確保稽核記錄機制已啟用，且依需求妥善設定稽核紀錄觸發政策(audit-policy-file 參數)，此政策可定義稽核紀錄日誌的產生條件(例如，紀錄時間週期、連線請求之行為觸發條件等相關設定)。若未啟用稽核紀錄機制或未妥善設定稽核紀錄觸發政策將無法有效產生紀錄，可能有無法追查及稽核問題之風險。並且稽核記錄日誌檔案與稽核紀錄觸發政策檔案權限設定為「擁有者能讀取與寫入、群組者能讀取、其他能讀取」，或更嚴格，避免遭非法存取修改之風險。

6.3.1.2 安全要求

(a) 應已設置適當的稽核記錄日誌路徑(audit-log-path 參數)

(b) 應依需求最小化設定稽核紀錄觸發政策(audit-policy-file 參數)

(c) 稽核記錄日誌檔案與稽核紀錄觸發政策檔案權限應設定為「擁有者能讀取與寫入、群組者能讀取、其他能讀取」，或更嚴格

6.4 資訊揭露 (Information disclosure)

6.4.1 ID01 應使用安全金鑰長度

6.4.1.1 指引說明

Kubernetes 建立加密 TLS 連線須以 PKI 憑證進行驗證，憑證驗證說明如下:

(a) Kubelet 以客戶端憑證至 API server 進行認證

(b) API server 以 Kubelet 伺服器端憑證與 Kubelets 通訊

(c) API server 以客戶端憑證與 Kubelets 通訊

(d) API server 以客戶端憑證與 etcd 通訊

(e) API server 端點之伺服器端憑證

(f) 叢集管理者以客戶端憑證至 API server 進行認證

(g) controller manager 以客戶端憑證與 API server 通訊

(h) scheduler 以客戶端憑證與 API server 通訊

(i) front-proxy 之伺服器端與客戶端憑證

因憑證為加密連線之重要依據。請檢視私密金鑰長度設定，建議 DSA 與 RSA 之非對稱加密演算法類型私密金鑰長度至少 2048 位元以上、ECDH 與 ECDSA 橢圓曲線密碼學（Elliptic Curve Cryptography，ECC）類型私密金鑰長度至少 224 位元及 AES 對稱金鑰演算法（Symmetric-key algorithm）鑰長度至少 128 位元，若使用長度不足之脆弱私密金鑰，可能存在加密連線遭破解之風險。

6.4.1.2 安全要求

(a) DSA 與 RSA 類型私密金鑰長度應至少 2048 位元以上

(b) ECDH 與 ECDSA 類型私密金鑰長度應至少 224 位元以上

(c) AES 類型私密金鑰長度應至少 128 位元以上

6.4.2 ID02 應強化設定金鑰管理存取權限

6.4.2.1 指引說明

建議應強化設定 Kubernetes 管理金鑰之存取權限，若存取權限設置不當，可能存在遭非法存取之風險。

6.4.2.2 安全要求

(a) pki 資料夾之檔案擁有者權限應設定為管理者權限

(b) pki 資料夾之憑證檔案權限應設定為「擁有者能讀取與寫入、群組者能讀取、其他能讀取」，或更嚴格

(c) pki 資料夾之金鑰檔案權限應設定為「擁有者能讀取與寫入、群組者無權限、其他無權限」，或更嚴格

6.4.3 ID03 TLS 密碼套件應使用安全之訊息鑑別碼演算法

6.4.3.1 指引說明

Kubernetes 建立加密 TLS 連線來加密保護傳輸之機敏資訊，而 TLS 所使用之密碼套件(Cipher suite)關係到加密保護強度。請檢視 TLS 密碼套件之訊息鑑別碼演算法(message authentication code (MAC) algorithm)設定，建議訊息鑑別碼演算法至少為 SHA-2 之 SHA-256，若使用加密強度不足之演算法，可能存在加密連線遭破解之風險。

6.4.3.2 安全要求

(a) TLS 密碼套件之訊息鑑別碼演算法應至少為 SHA-2 之 SHA-256

6.4.4 ID04 應避免預設不安全設定

6.4.4.1 指引說明

Kubernetes 以 namespace 提供一種用於叢集中進行資源群組隔離分配之機制，若使用 default 之 namespace 進行服務配置，可能有非法存取之風險。建議針對不同服務需求或類型，設定不同 namespace，強化與隔離存取權限之安全性。

6.4.4.2 安全要求

(a) 檢視執行中的 pod 應不得使用 default 之 namespace

6.4.5 ID05 應妥善設定重要檔案與資料夾存取權限

6.4.5.1 指引說明

管控 Kubernetes 重要設定檔案避免遭非擁有者惡意使用或竄改，建議 etcd、scheduler、controller-manager、API server 設定檔案之擁有者檔案權限設置為最高管理者，且其檔案存取權限設定為「擁有者能讀取與寫入、群組者能讀取、其他能讀取」，或更嚴格，若未妥善控管權限，可能有遭非法存取或系統異常之風險。

6.4.5.2 安全要求

(a) 確認 kube-apiserver.yaml 檔案權限設定應為「擁有者能讀取與寫入、群組者能讀取、其他能讀取」，或更嚴格

(b) 確認 kube-apiserver.yaml 擁有者檔案權限設定應為管理者權限

(c) 確認 kube-controller-manager.yaml 檔案權限設定應為「擁有者能讀取與寫入、群組者能讀取、其他能讀取」，或更嚴格

(d) 確認 kube-controller-manager.yaml 擁有者檔案權限設定應為管理者權限

(e) 確認 kube-scheduler.yaml 擁有者檔案權限設定應為管理者權限

(f) 確認 etcd.yaml 檔案權限設定應為「擁有者能讀取與寫入、群組者能讀取、其他能讀取」，或更嚴格

(g) 確認 etcd.yaml 擁有者檔案權限設定應為管理者權限

6.4.6 ID06 開啟最小化需求之網路服務

6.4.6.1 指引說明

Kubernetes 系統實際維運階段預設只執行原廠需要或自我宣告之網路協定與服務，確保於管理者知情下執行網路協定與服務，確保系統服務最小化之安全效益。建議 Kubernetes 系統管理者自我宣告預期開啟之網路協定與服務，系統上線後，建議檢視實際系統執行之網路協定與服務，以確保其一致性。

6.4.6.2 安全要求

(a) 應開啟自我宣告預期之網路協定與服務

(b) 應執行網路埠掃描，檢視實際系統執行之網路協定與服務，並與自我宣告一致

6.4.7 ID07 稽核紀錄保存管理

6.4.7.1 指引說明

檢視 Kubernetes 稽核紀錄之保存設定，若未妥善設定保存設定，可能有稽核紀錄遺失而無法鑑識確認事件發生根因之風險，建議設定 audit-log-maxage 確保最大稽核紀錄保存天數、audit-log-maxbackup 確保最大稽核紀錄保存檔案數及 audit-log-maxsize 確保稽核紀錄檔案上限大小(megabytes)。

6.4.7.2 安全要求

(a) 應設定 audit-log-maxage 參數

(b) 應設定 audit-log-maxbackup 參數

(c) 應設定 audit-log-maxsize 參數

6.5 阻斷服務 (Denial of Service)

6.5.1 DS01 應限制來自外部之異常連線或阻斷服務攻擊

6.5.1.1 指引說明

應防範限制來自外部之異常連線或阻斷服務攻擊，建議設定 enable-Admission-Plugins 之 EventRateLimit 參數來限制 API 服務之請求頻率，限制短時間大量連線至 API server 之異常連線，若未阻擋可能導致系統資源大量耗損或功能異常之風險。

6.5.1.2 安全要求

(a) 應設定 enable-Admission-Plugins 之 EventRateLimit 參數

6.6 提高特權 (Elevation of privilege)

6.6.1 EP01 避免共用預設 namespace

6.6.1.1 指引說明

預設 namespace 可能讓其他合法使用者濫用權限來存取機敏資料，若未妥善管理 pod 存取權限，可能有非法存取之風險。建議每個 pod 根據需求設定專屬 service account，避免使用預設 namespace，以達到使用資源隔離之安全性。

6.6.1.2 安全要求

(a) 應確認每個 pod 設定專屬 service account，及避免使用 default namespace

6.6.2 EP02 避免最高權限遭非法濫用

6.6.2.1 指引說明

因 Kubernetes 所處之作業系統之最高管理者擁有最高權限，可以存取或修改重要設定或機敏檔案，若未將最高管理者依需求作最小化設定，可能有遭最高管理者權限非法濫用之風險，建議確認具有最高管理者權限或可提權之帳號為符合最小需求。

6.6.2.2 安全要求

(a) 應確認具有最高管理者權限或可提權之帳號為符合最小需求

參考資料

(1) 3GPP TR 21.905-h10 Vocabulary for 3GPP Specifications (Release 17)
(https://www.3gpp.org/ftp/Specs/archive/21_series/21.905/21905-h10.zip)

版本修改紀錄

版本	時間	摘要
v1.0	2024/10/24	出版

地　址・台北市中正區北平東路30-2號6樓
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw