瞭解Cisco CEE可觀察性和Splunk整合

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

架構概觀

CEE名稱空間工作負載

CEE安裝和生命週期管理

- 安裝模式
- 定義CEE軟體專案
- 配置集群和運營中心
- 同步和驗證部署

CEE運營中心和運營管理

CEE可觀測性架構

Splunk整合：日誌傳送架構

Splunk HTTP事件收集器轉發

- HEC組態型號
- 捕獲HEC流量並對其進行故障排除

使用UDP 5140的系統日誌轉送

- RFC 5424欄位對映
- UDP傳輸和資料包捕獲

警報、SNMP和CIMC可觀察性

批次統計資料

OpenTelemetry System Gateway

- 系統閘道型號
- 閘道組態概念
- 遠端匯出器
- 與OpenShift OpenTelemetry比較

驗證設定

- 驗證CEE同步
- 分別檢驗HEC和系統日誌
- 驗證可觀察服務

預期行為

決策流程

結論

相關內容

簡介

本檔案介紹思科通用執行環境(CEE)架構、部署、監控、Splunk整合和OpenTelemetry。

必要條件

需求

思科建議熟悉以下技術：

- 雲原生部署平台(CNDP)、Kubernetes名稱空間和Pod放置。
- 思科使用者微服務基礎設施(SMI)和SMI集群管理器。
- CEE運營中心、Prometheus、Grafana、Alertmanager和日誌轉發元件。
- 使用tcpdump執行Splunk HTTP Event Collector(HEC)、系統日誌和資料包捕獲。
- OpenTelemetry Protocol(OTLP)和OpenTelemetry Collector，用於較新的網關整合。

採用元件

示例顯示一個基於Kubernetes的Cisco SMI/CNDP環境，其中包含CEE和關聯的會話管理功能(SMF)應用程式。軟體定義示例是指CEE包2026.01.1.08;「運營中心」示例使用SMF儲存庫識別符號smf-2026.04.m0.i50。這些是示例值，而不是部署要求。

必須將網路端點、群集名稱和名稱空間值替換為目標部署所認可的值。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

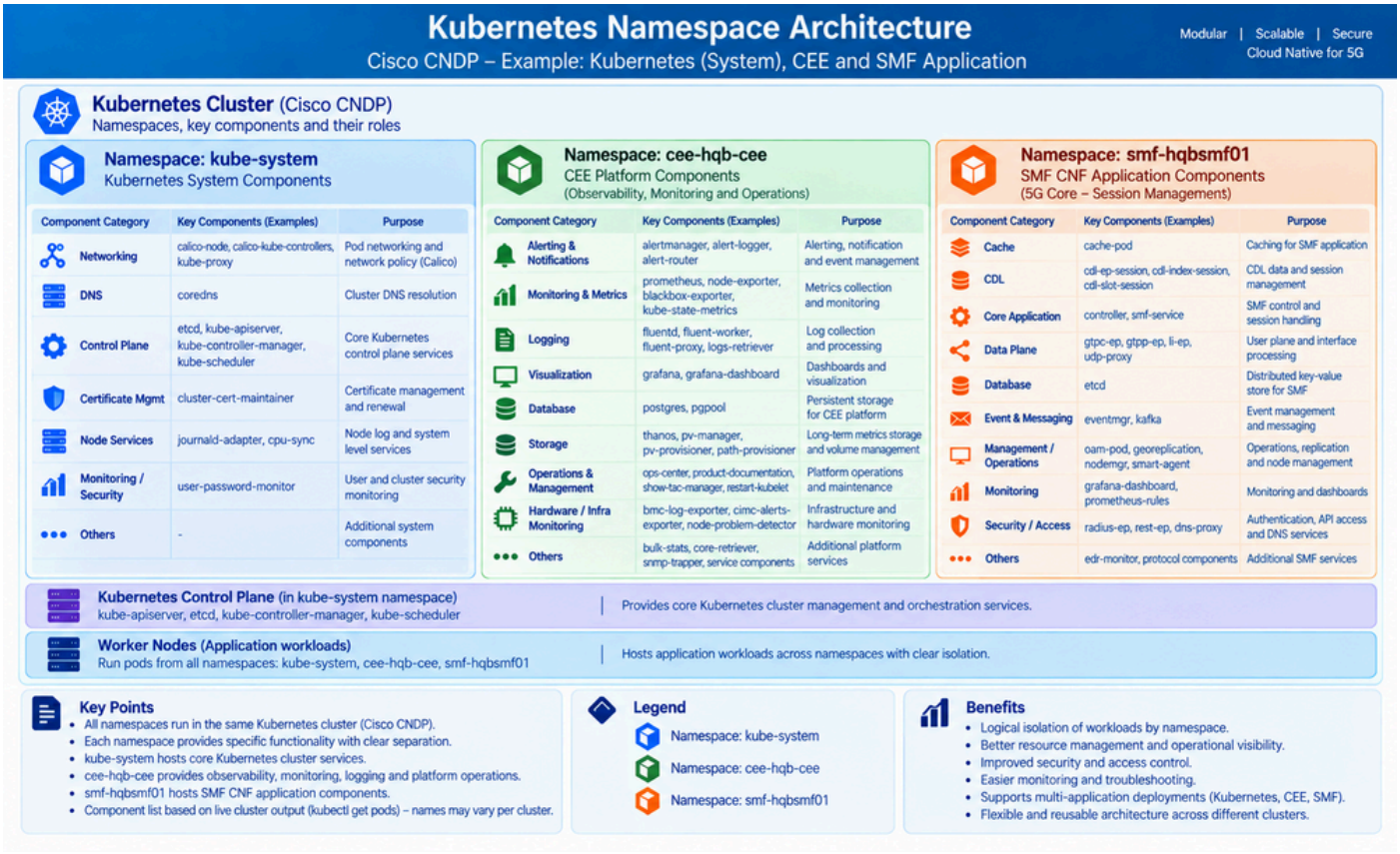
思科通用執行環境(CEE)是思科使用者微服務基礎設施(SMI)的一部分。 在基於Kubernetes的CNDP部署中，Kubernetes名稱空間獨立平台服務、CEE可觀察性和Kubernetes管理服務以及SMF應用工作負載。分離提供了管理和操作邊界，而Kubernetes網路和服務發現允許元件通訊。

本文檔涵蓋名稱空間架構、CEE工作負載、CEE安裝和生命週期管理、CEE運營中心、警報和簡單網路管理協定(SNMP)、思科整合管理控制器(CIMC)警報、日誌轉發、批次統計資料和OpenTelemetry系統網關。

傳輸控制通訊協定(TCP)連線埠8088上的HEC和使用者資料包通訊協定(UDP)連線埠5140上的系統日志是獨立的攝取機制。兩條路徑具有不同的配置、傳輸和故障排除要求，可以共存。

架構概觀

CEE和關聯的應用程式函式佔據單獨的Kubernetes名稱空間。該架構將Kubernetes平台服務與CEE可觀察性和管理功能以及SMF應用領域區分開來。



顯示CEE和應用平台分離的Cisco SMI名稱空間架構

CEE名稱空間是服務級別體系結構的主要焦點。其他名稱空間提供Kubernetes平台、網路功能和SMF工作負載。

CEE名稱空間工作負載

CEE名稱空間託管用於監控、警報、記錄、儀表板、統計和操作訪問的微服務。

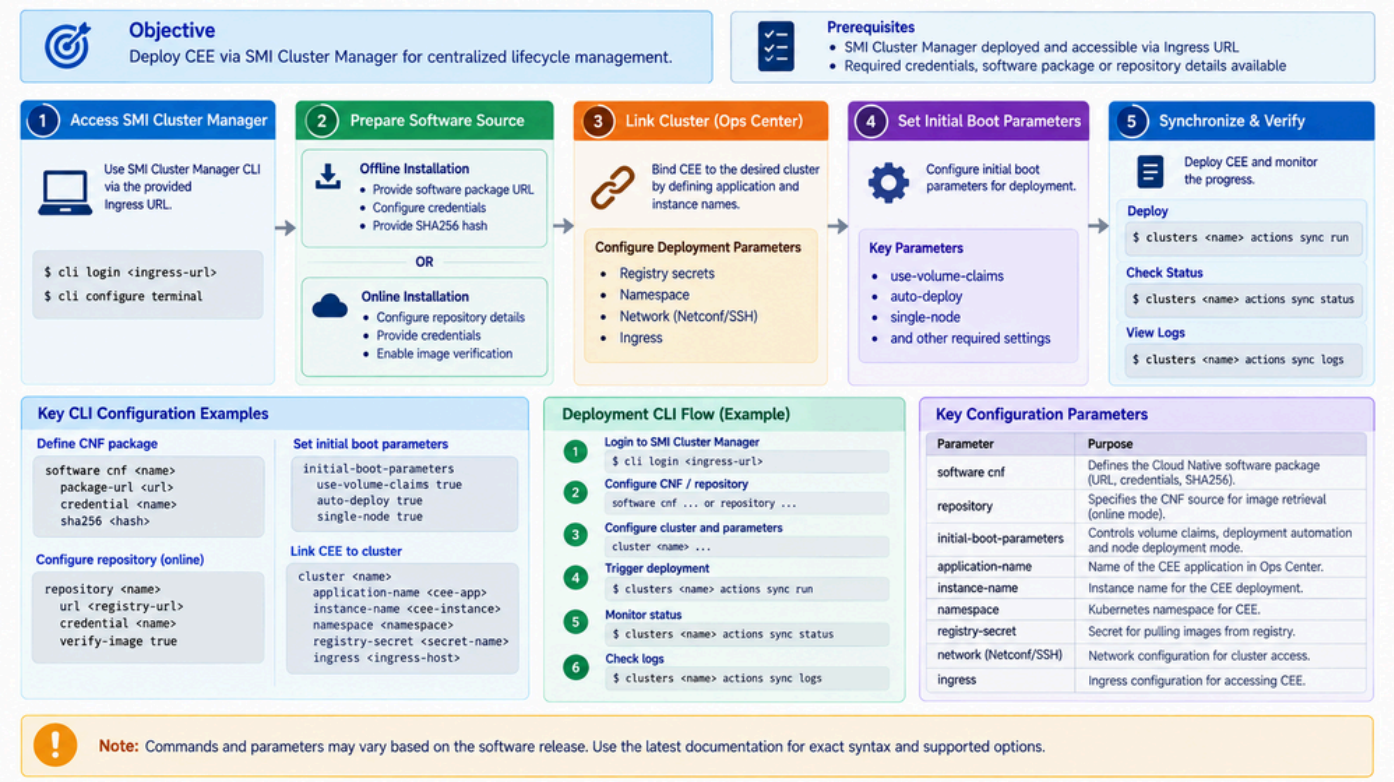


CEE名稱空間微服務及其操作工作負載的功能

這些功能包括Prometheus度量收集、Grafana視覺化、Alertmanager警報處理、日誌轉發服務和定期批次統計建立。各個工作負載因版本和部署配置而異。

CEE安裝和生命週期管理

SMI群集管理器將軟體對象定義與目標群集及其運營中心配置分隔開來。這實現了受控軟體版本和可重複的集群同步。



SMI Cluster Manager CEE安裝和軟體同步架構

安裝模式

- 離線安裝可以通過檔案URL和256位安全雜湊演算法(SHA-256)雜湊引用本地軟體包。
- 群集配置將CEE/SMF部署與預期的群集和Ops Center例項相關聯。

定義CEE軟體專案

在SMI Cluster Manager配置中，識別本地CEE軟體包及其SHA-256雜湊。

```
software cnf cee
  url file:///data/software/images/cee-2026.01.1.08.tar
  sha256 <CEE-SHA256-HASH>
exit
```

使用批准的包中的精確SHA-256值。命令中的佔位符是有意的，並不表示實際的校驗和。

配置集群和運營中心

源配置將群集與SMF運營中心、本地儲存庫、管理端點和部署設定相關聯。站點特定的識別符號由

佔位符替換。

```
clusters <cluster-name>
  ops-centers smf <smf-ops-center-name>
    app-name-override cn
    repository-local smf-2026.04.m0.i50
    sync-default-repository true
    netconf-ip <NETCONF-IP>
    netconf-port 2029
    ssh-ip <SSH-IP>
    ssh-port 2028
    initial-boot-parameters use-volume-claims true
    initial-boot-parameters auto-deploy false
    initial-boot-parameters single-node false
  exit
exit
```

參數	示例配置中的含義
ops-centers smf <smf-ops-center-name>	將群集與SMF Ops Center例項相關聯。
repository-local	指定用於部署的應用程式儲存庫和版本。
sync-default-repository true	在同步期間使用配置的預設儲存庫。
netconf-port 2029	指定NETCONF管理連線埠。
ssh-port 2028	指定安全外殼(SSH)管理連線埠。
use-volume-claims true	允許使用卷宣告來滿足持久儲存要求。
自動部署false	禁用自動部署，以便同步和驗證仍由顯式控制。
單節點false	指定不處於單節點模式的部署。



附註：包和系統資訊庫識別符號是源配置中的示例。在其他群集中使用版本相容性和終結點值之前，請確認這些值。

同步和驗證部署

在軟體和Ops Center配置準備就緒後運行群集同步操作。

```
clusters <cluster-name> actions sync run
```

檢查同步狀態和日誌。

```
clusters <cluster-name> actions sync status
clusters <cluster-name> actions sync logs
```

確認同步已成功完成，並且已部署預期的CEE Pod和服務。

⚠ 注意：群集同步和軟體部署可以改變運行環境。根據批准的維護和部署流程應用更改。

CEE運營中心和運營管理

CEE Ops Center為CEE服務提供操作介面。該工作負載支援集群內CEE功能的使用者管理、身份驗證、配置和show命令。SMI群集管理器通過管理配置將Ops Center與目標部署相關聯。

運營中心屬於管理平面。Prometheus、Alertmanager、Fluent Bit/fluent-proxy、HEC、syslog和OpenTelemetry屬於監控和遙測路徑。將這些責任分離開來，可簡化故障排除。

CEE可觀測性架構

CEE可觀察性包括度量、警報、日誌、CIMC警報和批次統計資料。這些服務是相關的，但資料路徑和使用者不同。

功能	主要用途	典型目的地或消費者
指標	從節點、Kubernetes和服務收集並查詢時間系列測量值。	普羅米修斯，格拉法納和薩諾斯。
警報	評估警報規則並路由警報事件。	Alertmanager、alert-router、Ops Center和外部接收器。
記錄檔	將日誌和事件記錄轉發到外部收集器或後端。	Splunk和其他日誌收集器。
CIMC警報	匯出思科整合管理控制器警報以進行監控。	CEE指標/警報和Grafana。
批次統計資料	建立定期統計快照。	CSV快照和下游處理或分析。

Splunk整合：日誌傳送架構

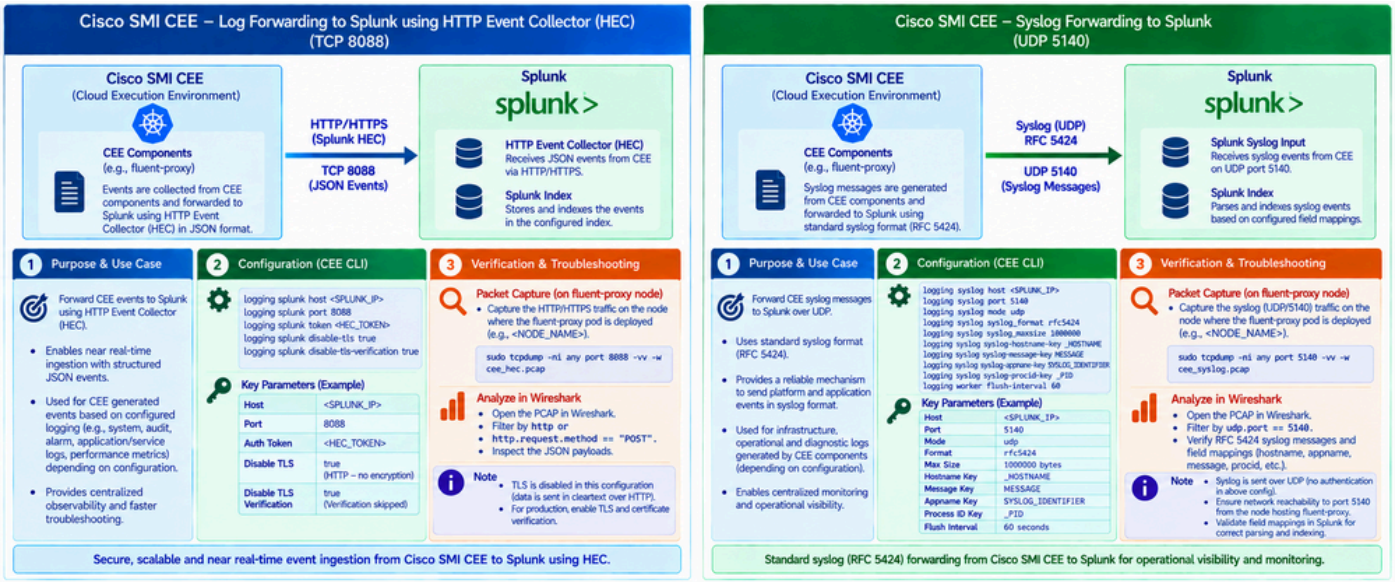
來源說明兩個CEE到Splunk的路徑。兩者都可以向Splunk傳送事件，但是它們使用不同的協定和接收介面。

```
CEE
  |-- logging splunk --> HEC / TCP 8088 --> Splunk HEC input
```

```
|
+-- logging syslog --> RFC 5424 / UDP 5140 --> Splunk syslog input
```

每條路徑所承載的事件型別取決於CEE配置和實施的轉發管道。兩個配置的介面未確定每個介面都包含互斥的事件類別。

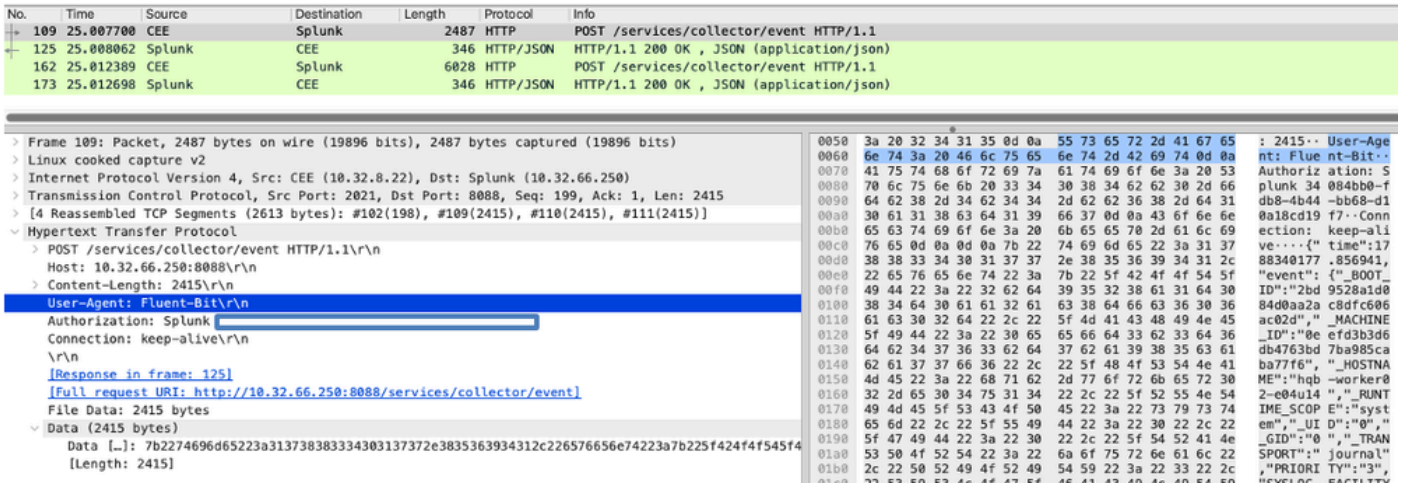
分別追蹤路徑。成功的HEC傳遞不會確認系統日誌傳遞，而成功的系統日誌傳遞不會確認HEC傳遞。



CEE Splunk與單獨的HEC和syslog轉發路徑整合

Splunk HTTP事件收集器轉發

Splunk HEC接受HTTP事件提交並使用HEC身份驗證令牌。CEE將事件直接轉發到已配置的HEC服務，而不是要求對此路徑進行基於檔案的接收。



HEC組態型號

原始實驗示例包含這些CEE Splunk端點設定。該摘錄記錄了源行為，並不是推薦的生產配置。

⚠ 注意：源示例同時禁用TLS和證書驗證。這會使遙測和HEC憑證在網路上被攔截。對於生產，請根據支援的CEE版本配置啟用TLS和證書驗證並保護HEC身份驗證令牌。

```
logging splunk
  <CEE-specific HEC endpoint and authentication parameters>
  disable-tls true
  disable-tls-verification true
```

在源體系結構中，CEE日誌/事件生成器通過相關的Fluent轉發元件轉發到HEC目的地。

```
CEE log or event source
  |
  v
CEE forwarding service / fluent-proxy
  |
  +-- HTTP(S) HEC over TCP 8088 --> Splunk HEC endpoint
                                       |
                                       v
                                Splunk ingestion tier
                                       |
                                       v
                                Splunk indexing tier
```

捕獲HEC流量並對其進行故障排除

當fluent-proxy承載HEC流量時，在CEE名稱空間中識別fluent-proxy pod及其Kubernetes工作節點。

```
kubectl get pods -n <cee-namespace> -o wide | grep fluent-proxy
```

在傳輸HEC流量的Kubernetes節點上，捕獲HEC埠的資料包。

```
tcpdump -ni any port 8088 -vv -w splunk_hec.pcap
```

對於啟用TLS的連線，資料包捕獲會顯示傳輸建立和目標詳細資訊，但通常不會顯示HTTP負載。如果禁用了TLS，則可以在捕獲中看到事件內容和身份驗證資料。

⚠ 注意：資料包捕獲和日誌可能包含敏感的遙測和憑據。限制對授權支援工作流的收集和傳輸，並保護捕獲檔案。

使用UDP 5140的系統日誌轉送

第二個Splunk整合路徑使用RFC 5424格式設定和UDP埠5140轉發系統日誌記錄。源配置還定義欄位對映、最大消息大小和工作器刷新間隔。

```
logging syslog host <SPLUNK-IP>
logging syslog port 5140
logging syslog mode udp
logging syslog syslog_format rfc5424
logging syslog syslog_maxsize 1000000
logging syslog syslog-hostname-key _HOSTNAME
logging syslog syslog-message-key MESSAGE
logging syslog syslog-appname-key SYSLOG_IDENTIFIER
logging syslog syslog-procid-key _PID
logging worker flush-interval 60
```

RFC 5424欄位對映

CEE源欄位	系統日誌欄位或用途
主機名(_O)	在生成的系統日誌記錄中標識源主機。
訊息	傳送日誌消息正文。
系統日誌識別符號	提供系統日誌應用程式或程式識別符號。
PID(_P)	攜帶源進程識別符號。

UDP傳輸和資料包捕獲

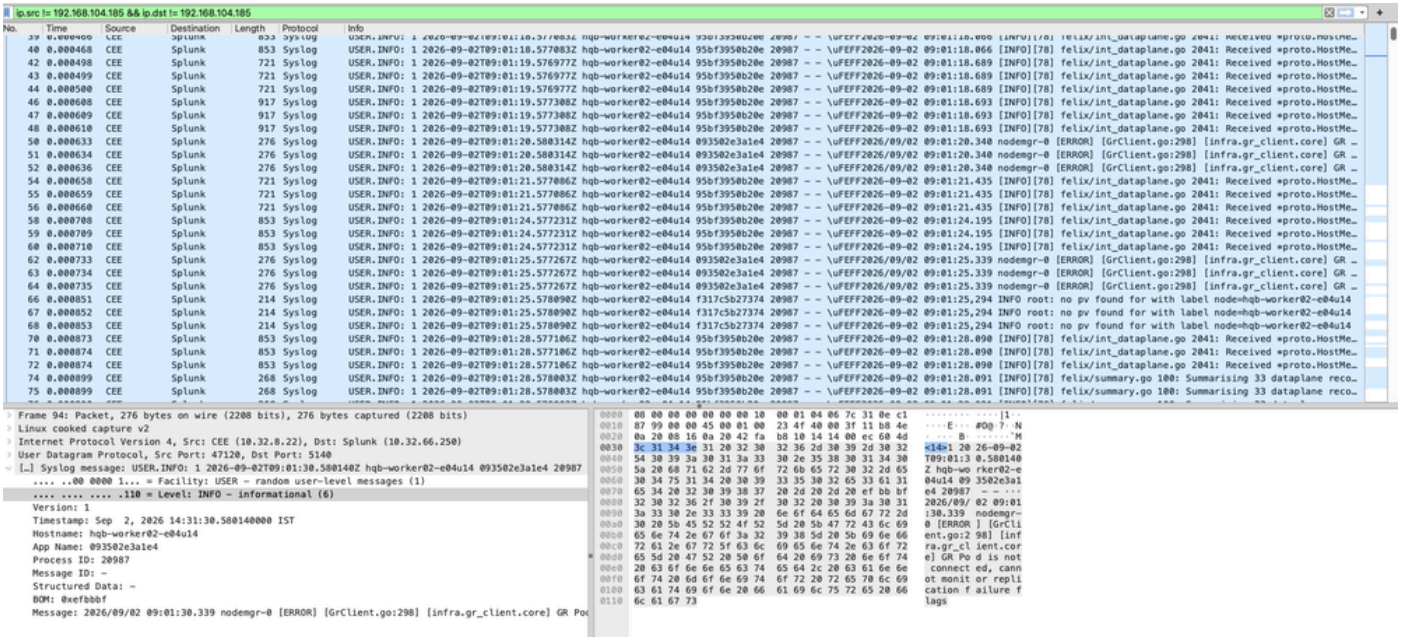
UDP是無連線協定，既不提供傳輸交付確認，也不提供重傳。故障排除必須考慮資料包丟失、路由、最大傳輸單元(MTU)、分段、接收方可用性和隊列/速率行為。

在傳輸系統日誌流量的介面或Kubernetes節點上，運行：

```
tcpdump -ni any udp port 5140 -vv -w splunk_syslog.pcap
```

如果Fluent-Proxy轉發系統日誌流量，則託管該元件的節點是合適的資料包捕獲點。收集封包之前驗證轉送路徑。

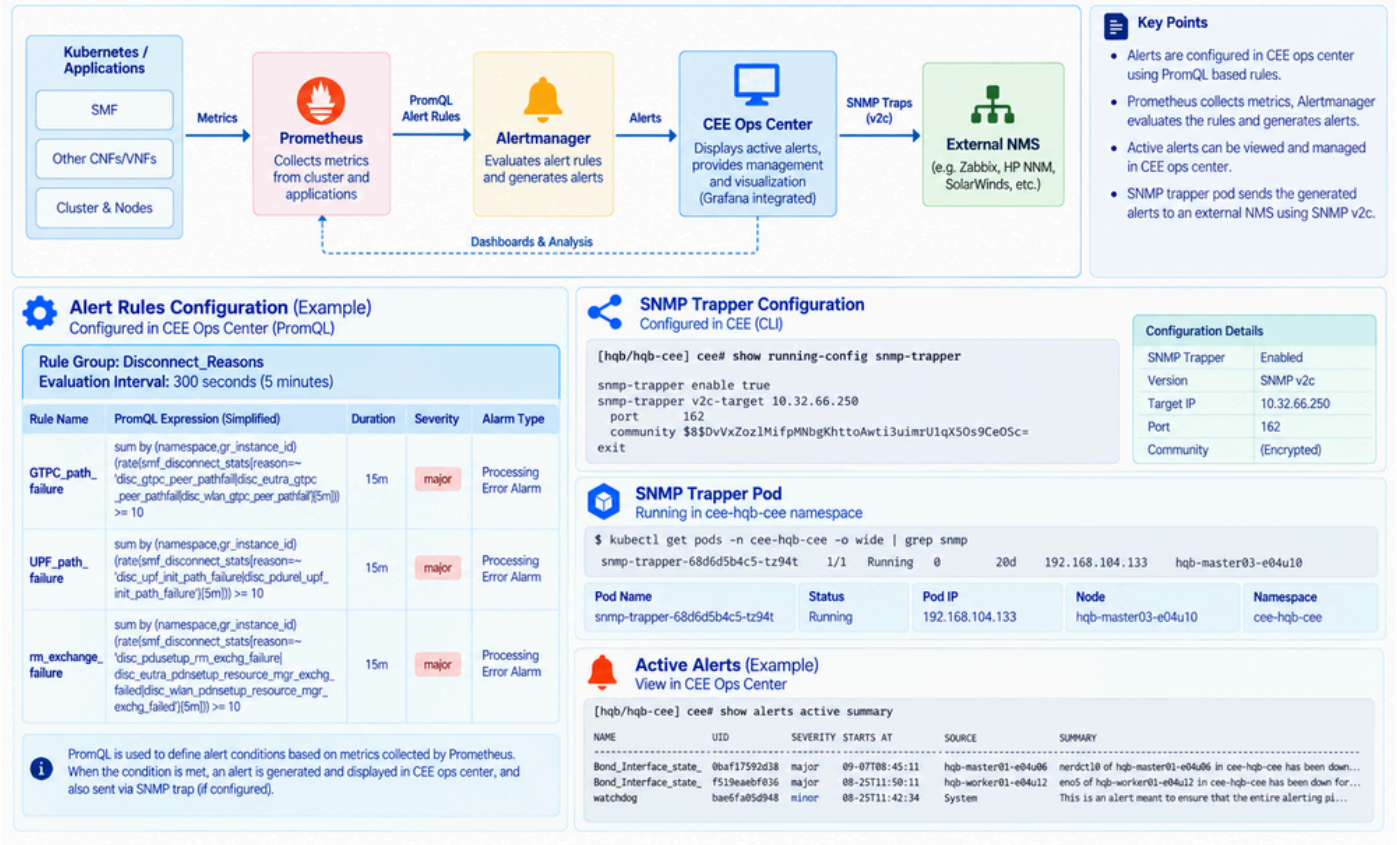
附註：RFC 5424定義獨立於選定傳輸的系統日誌消息格式。源方案使用UDP 5140。基於TLS的系統日誌傳輸是一個不同的選項，它需要相容的傳送者和接收者配置。



使用UDP埠5140和RFC 5424欄位將CEE系統日誌轉發到Splunk

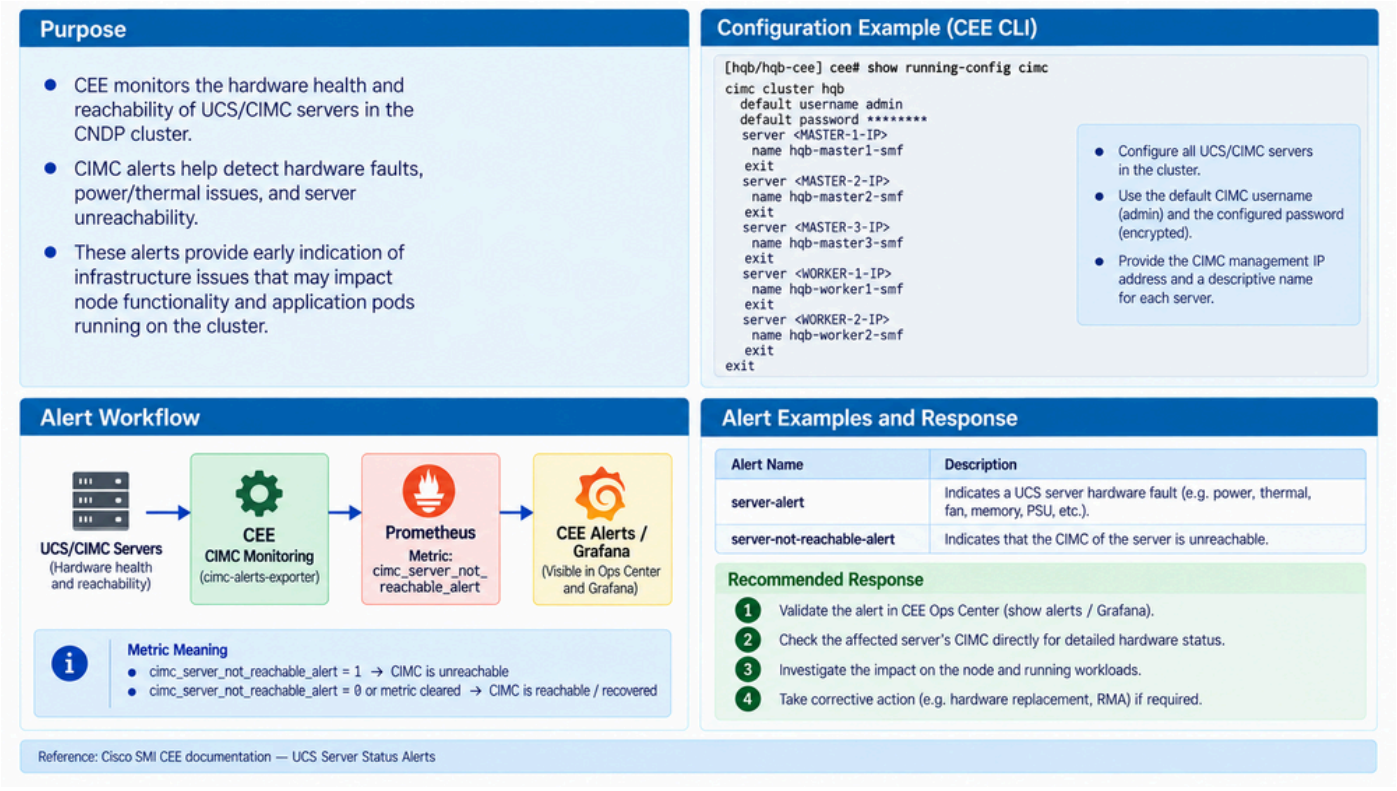
警報、SNMP和CIMC可觀察性

CEE警報使用Prometheus和Alertmanager。Prometheus評估指標和警報規則。Alertmanager將警報事件路由到接收器，並且警報路由器提供額外的路由支援。CEE警報記錄器提供歷史警報記錄，以便通過CEE運營中心進行檢索。



CEE Prometheus和Alertmanager警報轉發和SNMP架構

CIMC警報整合提供了相關的基礎設施監控路徑。cimc-alerts-exporter將收集CIMC警報資訊並公開該資訊，以便在Grafana中進行監控和視覺化。



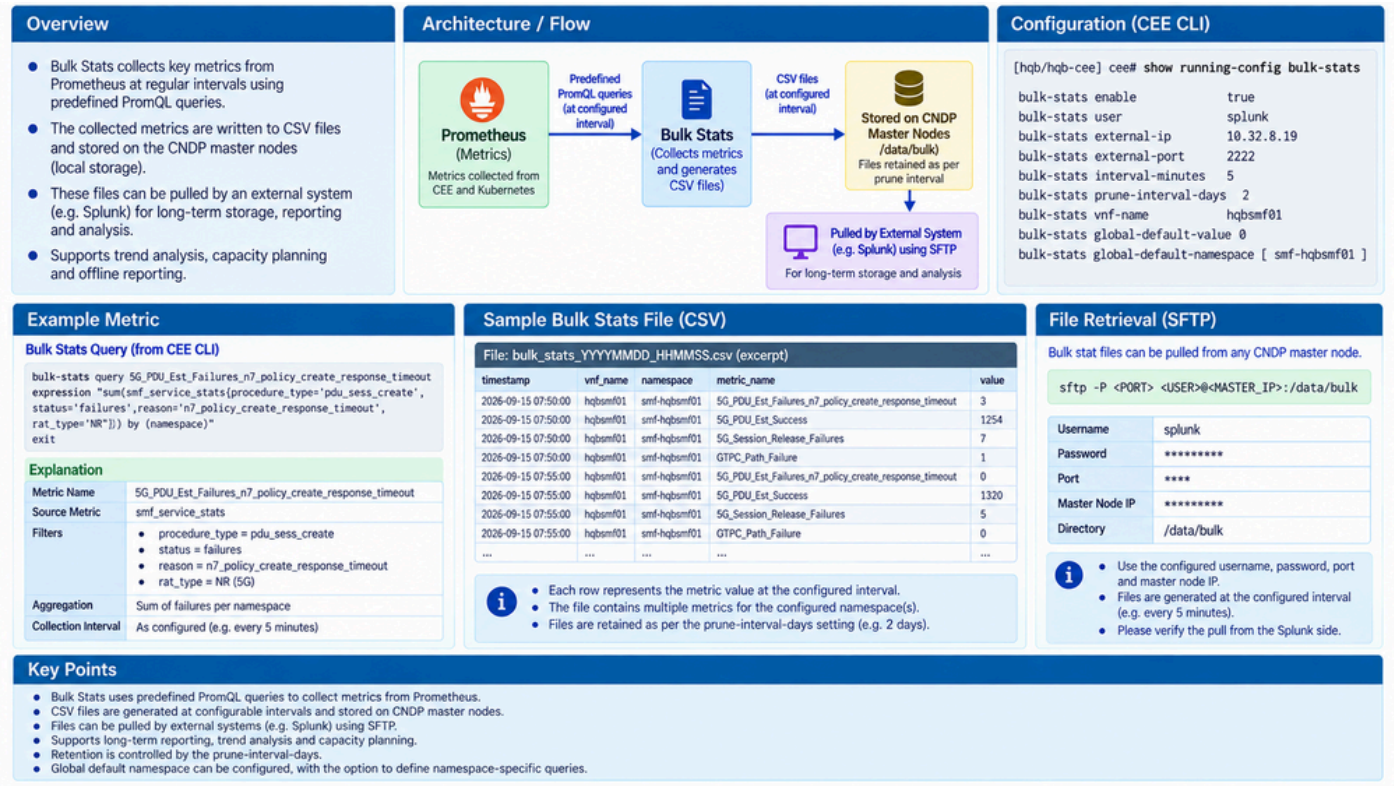
CEE CIMC警報匯出器與監控控制面板整合

SNMP整合是一個警報和管理介面；它不能與Splunk HEC或系統日誌轉發互換。協定和事件傳送路徑仍然不同。

相關管理資訊庫(MIB)參考包括CISCO-CNEE-MIB.my和CISCO-SMI.my。

批次統計資料

CEE bulk-stats服務建立通過Prometheus收集的統計資訊的定期逗號分隔值(CSV)快照。這些是統計快照，而不是應用程式日誌記錄流。



CEE批次統計服務根據Prometheus度量建立定期CSV快照

Bulk-statistics輸出支援定期報告、趨勢分析和下游資料處理。僅當部署明確將CSV/統計資訊資料轉發或匯入到Splunk時，才將其包括在Splunk整合路徑中。

OpenTelemetry System Gateway

較新的Cisco SMI版本支援平台管理的OpenTelemetry Collector網關。網關通過OpenTelemetry Protocol(OTLP)從應用接收遙測，並將支援的度量和日誌轉發到本地或遠端後端。

附註：Cisco SMI Cluster Manager Operations文檔識別OpenTelemetry網關與版本2026.03.1的整合。網關未在源示例描述的特定部署中驗證，因此本節介紹已發佈的配置模型，而不是該環境中的已驗證操作。

系統閘道型號

```
OpenTelemetry-enabled applications
        |
        | OTLP
        v
CEE OpenTelemetry System Gateway
        |
        +--> Local metrics backend
        +--> Local logging backend
        +--> Remote exporters
                 |
                 +--> OTLP / OTLPHTTP
                 +--> Splunk HEC
                 +--> Other supported destinations
```

閘道組態概念

啟用OpenTelemetry Collector網關並選擇本地度量和日誌後端。

```
otel-collector gateway enabled
otel-collector gateway system local-backends metrics-enabled true
otel-collector gateway system local-backends logs-enabled true
```

當部署需要外部服務暴露時，配置可以包括外部IP。

```
otel-collector gateway system external-ip <external-ip-address>
```

為網關匯出器配置了可選的代理設定。

```
otel-collector gateway system proxy http-proxy http://<proxy-host>:<proxy-port>
otel-collector gateway system proxy https-proxy http://<proxy-host>:<proxy-port>
otel-collector gateway system proxy no-proxy 127.0.0.1,.svc,.cluster.local
```

本地後端選項控制平台管理的系統網關向內建後端傳送遙測的方式。外部IP暴露和代理設定取決於拓撲和安全要求。

遠端匯出器

匯出器	訊號	技術用途
otlp	日誌，度量	將遙測傳送到接受OTLP over gRPC的後端。
otlphttp	日誌，度量	將遙測傳送到通過HTTP接受OTLP的後端。
斯普林赫克	記錄檔	將日誌傳送到Splunk HEC終結點。
日記本	記錄檔	將日誌寫入支援的節點日誌。
debug	日誌，度量	支援受控驗證和故障排除。

OpenTelemetry管道遵循接收、處理和匯出模型。接收方接收遙測；處理器過濾或轉換資料；匯出器將所選訊號傳送到遠端或本地後端。

來源還區分代理行為：otlp使用收集器例項代理設定，而otlphttp和splunkhec支援匯出器級代理覆蓋，其中部署的版本公開了該配置。

與OpenShift OpenTelemetry比較

Cisco CEE和OpenShift具有共用架構模式：OpenTelemetry Collector可以位於儀表式應用和可觀察性後端之間。它們的管理和安裝模式不同。

概念	CEE OpenTelemetry系統網關	OpenShift OpenTelemetry模式
遙測源	支援OpenTelemetry的CEE和應用工作負載	支援OpenTelemetry的OpenShift工作負載
通訊協定	OTLP	OTLP
收集器角色	平台管理的系統網關	OpenTelemetry Collector部署或例項
管道概念	接收、處理、匯出	接收、處理、匯出
後端靈活性	本地後端和支援的遠端匯出器	匯出器驅動後端整合
Splunk整合	文檔化的CEE配置中的splunkhec匯出器	Splunk HEC匯出器（配置時）

這種比較是架構性的。這兩個平台並未宣稱以相同方式實現OpenTelemetry。OpenShift通常使用OpenTelemetry操作員/收集器部署模式，而Cisco SMI系統網關是平台管理的。

源中討論的OpenShift參考架構顯示收集器通過HEC從Kubernetes工作負載向Splunk轉發遙測資料。它說明了基於收集器的模型，而不是針對樣例CEE安裝的經驗證的整合。

驗證設定

驗證CEE同步

檢查SMI Cluster Manager同步狀態和日誌，並確認已部署預期的CEE工作負載。

```
clusters <cluster-name> actions sync status
clusters <cluster-name> actions sync logs
```

分別檢驗HEC和系統日誌

確認HEC路徑將事件傳送到配置的TCP 8088端點並且Splunk收到這些事件。分別確認系統日誌路徑將UDP 5140記錄傳送到配置的監聽程式。

使用相應部分中的資料包捕獲方法，並將資料包時間戳與已配置的收集器上接收的事件相關聯。

驗證可觀察服務

確認指標、警報路由、CIMC警報和批次統計資料快照按照針對已安裝版本設計的操作方式運行。如果啟用OpenTelemetry，請使用支援的SMI Cluster Manager操作過程驗證接收器、管道和匯出器運行狀況。

預期行為

元件或路徑	預期結果
SMI叢集管理員	集群同步完成，並且部署所需的CEE服務。
運營中心	授權使用者可以訪問操作功能和支援的配置/監控命令。
Splunk HEC	事件流量到達TCP埠8088上配置的HEC偵聽程式。
系統日誌	RFC 5424格式的事件到達配置的UDP埠5140監聽程式。
警報和CIMC	Alertmanager和相關匯出器顯示已配置的警報資訊。
批次統計資料	根據收集到的統計資訊生成定期CSV快照。
OpenTeletry	在配置了網關的受支援版本中，OTLP訊號流經選定的後端/匯出器管道。

決策流程

觀察	下一檢查
同步後沒有CEE服務。	檢查Cluster Manager同步狀態、日誌、軟體專案和Ops Center引數。
缺少HEC事件。	識別轉發池/節點，驗證TCP 8088流量、HEC目標、身份驗證和TLS配置。
缺少系統日誌事件。	驗證UDP 5140目的地、RFC 5424格式、封包流和接收器行為。

觀察	下一檢查
缺少警報或CIMC資料。	檢查Prometheus/Alertmanager路由、alert-router和cimc-alerts-exporter操作。
缺少批次統計資料。	確認批次統計服務操作、Prometheus資料可用性和CSV快照生成。
缺少OpenTelemetry匯出。	驗證已安裝版本、網關配置、接收器和匯出器狀態以及管道成員資格的功能支援。

結論

CEE是一個基於Kubernetes的分層執行和可觀察環境，圍繞SMF應用。Kubernetes名稱空間分離將平台操作、CEE服務和應用工作負載劃分到不同的域。在CEE中，監控、警報、日誌記錄和批次統計資料是具有獨立職責的專門服務。

Splunk的關鍵區別在於使用TCP 8088的HEC和使用UDP 5140的syslog。以下是具有不同協定、配置和故障排除過程的單獨轉發路徑。較新的OpenTelemetry系統網關新增了基於OTLP的收集器和匯出器模型。它與OpenShift OpenTelemetry的相似之處是架構性的，並且必須針對特定的CEE發佈和部署驗證網關操作。

相關內容

- Cisco CEE配置和管理指南 — 通用執行環境
- Cisco CEE配置和管理指南 — 日誌記錄命令
- Cisco SMI Cluster Manager操作 — 同步和OpenTelemetry
- RFC 5424 — 系統日誌協定

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。