了解Cisco CEE可观察性和Splunk集成

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

体系结构概述

CEE命名空间工作负载

CEE安装和生命周期管理

- 安装模式
- 定义CEE软件对象
- 配置集群和运营中心
- 同步和验证部署

CEE运营中心和运营管理

CEE可观测性架构

Splunk集成：日志传输架构

Splunk HTTP事件收集器转发

- HEC配置模型
- 捕获HEC流量并对其进行故障排除

通过UDP 5140的系统日志转发

- RFC 5424字段映射
- UDP传输和数据包捕获

警报、SNMP和CIMC可观察性

批量统计数据

OpenTelemetry系统网关

- 系统网关型号
- 网关配置概念
- 远程导出器
- 请比较OpenShift OpenTelemetry

检查配置

- 验证CEE同步
- 分别验证HEC和系统日志
- 检验可观察服务

预期行为

决策流程

结论

相关内容

简介

本文档介绍思科通用执行环境(CEE)架构、部署、监控、Splunk集成和OpenTelemetry。

先决条件

要求

思科建议熟悉以下技术：

- 云原生部署平台(CNDP)、Kubernetes命名空间和Pod放置。
- 思科用户微服务基础设施(SMI)和SMI集群管理器。
- CEE运营中心、Prometheus、Grafana、Alertmanager和日志转发组件。
- 使用tcpdump执行Splunk HTTP事件收集器(HEC)、系统日志和数据包捕获。
- OpenTelemetry Protocol(OTLP)和OpenTelemetry Collector，用于较新的网关集成。

使用的组件

示例展示基于Kubernetes的Cisco SMI/CNDP环境，其中包含CEE和关联的会话管理功能(SMF)应用。软件定义示例是指CEE包2026.01.1.08;运营中心示例使用SMF存储库标识符smf-2026.04.m0.i50。这些是示例值，不是部署要求。

网络终端、群集名称和命名空间值必须替换为目标部署所批准的值。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

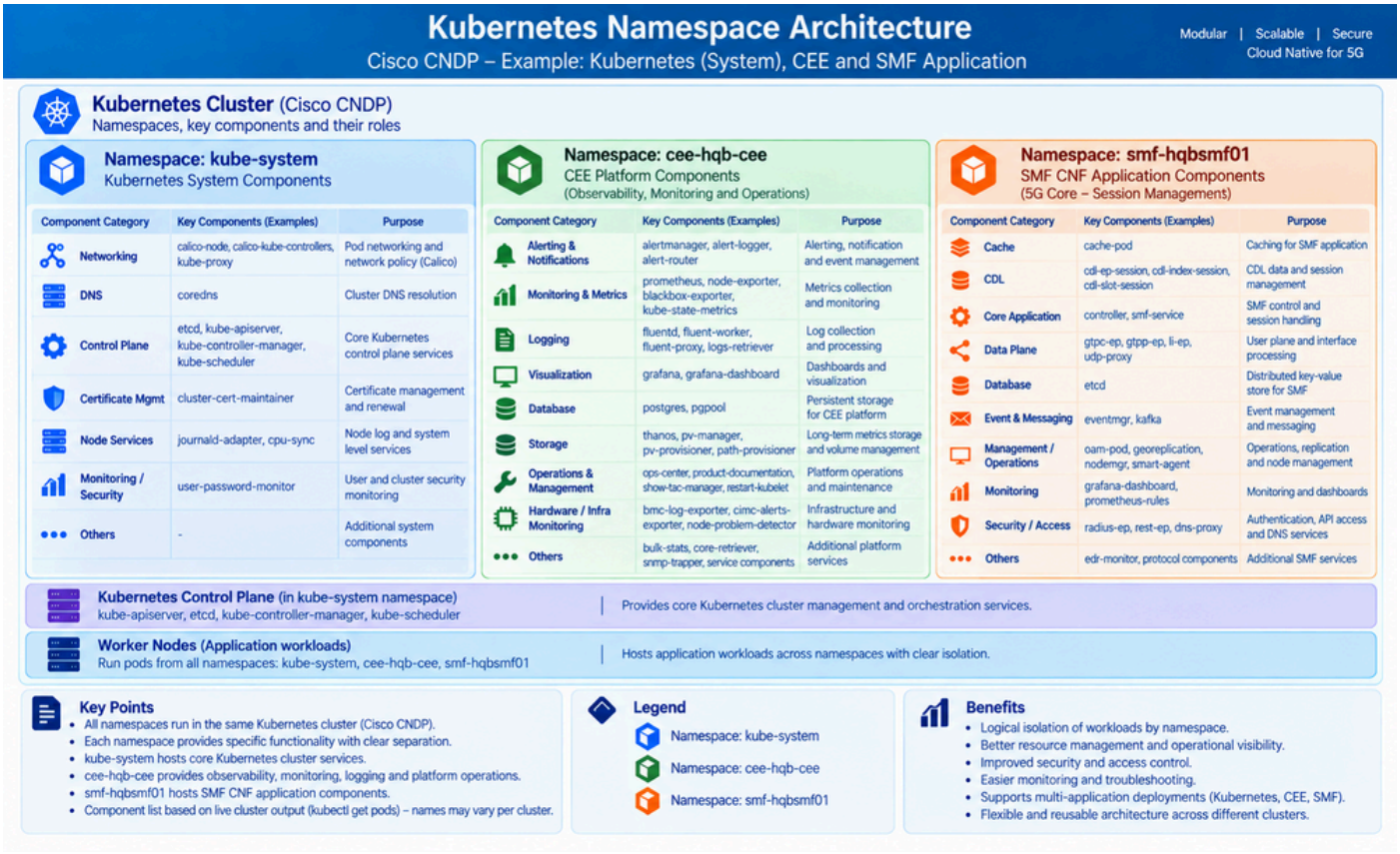
Cisco Common Execution Environment(CEE)是Cisco Subscriber Microservices Infrastructure(SMI)的一部分。 在基于Kubernetes的CNDP部署中，Kubernetes名称空间提供单独的平台服务、CEE可观察性和Kubernetes管理服务以及SMF应用工作负载。分离提供了管理和操作边界，而Kubernetes网络和服务发现允许组件通信。

本文档涵盖命名空间架构、CEE工作负载、CEE安装和生命周期管理、CEE运营中心、警报和简单网络管理协议(SNMP)、思科集成管理控制器(CIMC)警报、日志转发、批量统计数据和OpenTelemetry系统网关。

传输控制协议(TCP)端口8088上的Splunk HEC和用户数据报协议(UDP)端口5140上的系统日志是独立的接收机制。这两条路径具有不同的配置、传输和故障排除要求，并且可以共存。

体系结构概述

CEE和相关应用功能占用单独的Kubernetes命名空间。该架构将Kubernetes平台服务与CEE可观察性和管理功能以及SMF应用领域区分开来。



显示CEE和应用平台分离的Cisco SMI命名空间架构

CEE命名空间是服务级别体系结构的重点。其他命名空间提供Kubernetes平台、网络功能和SMF工作负载。

CEE命名空间工作负载

CEE命名空间托管用于监控、警报、日志记录、控制面板、统计信息和操作访问的微服务。

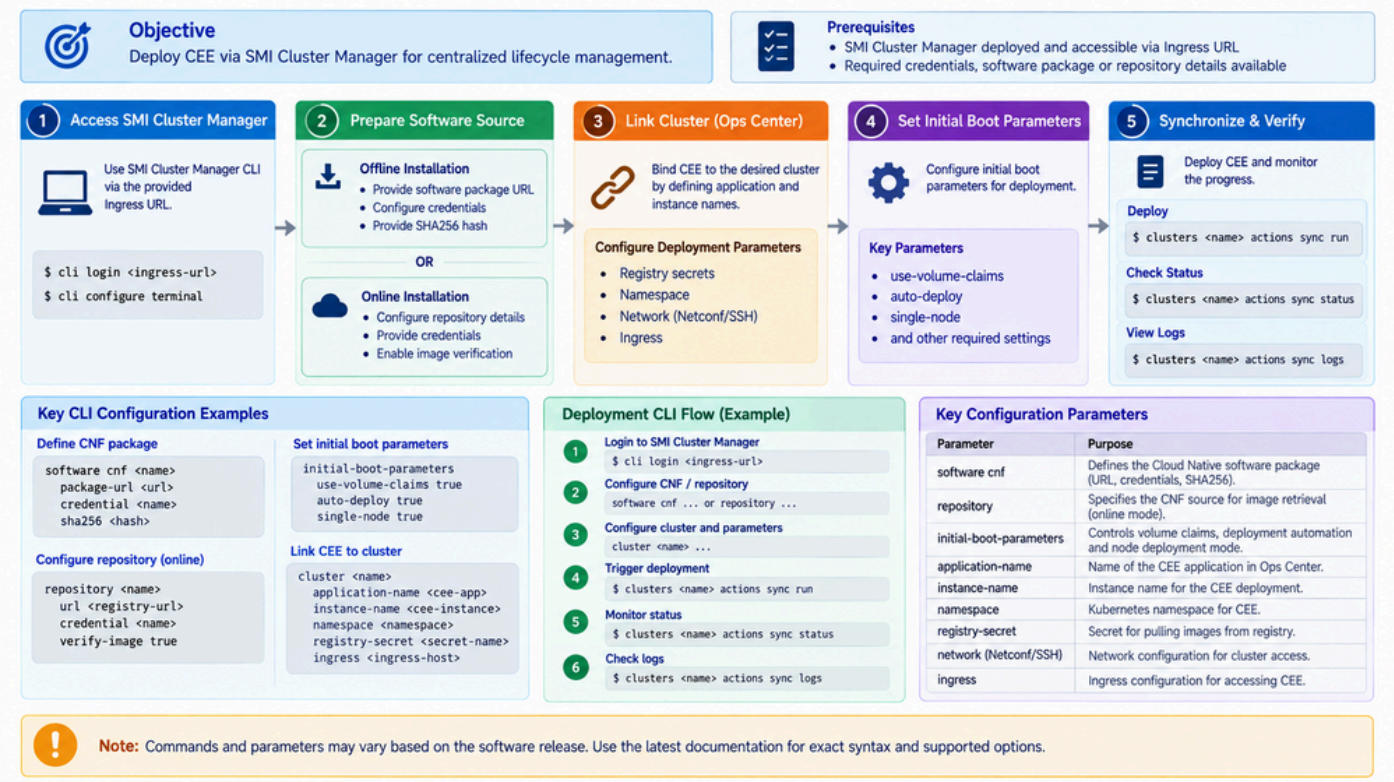


CEE命名空间微服务及其操作工作负载的功能

这些功能包括Prometheus指标收集、Grafana可视化、Alertmanager警报处理、日志转发服务和定期批量统计数据创建。各个工作负载因版本和部署配置而异。

CEE安装和生命周期管理

SMI群集管理器将软件对象定义与目标群集及其运营中心配置分开。这实现了受控软件版本和可重复的集群同步。



SMI Cluster Manager CEE安装和软件同步架构

安装模式

- 脱机安装可以通过文件URL和256位(SHA-256)安全散列算法来引用本地软件包。
- 集群配置将CEE/SMF部署与预期的集群和运营中心实例相关联。

定义CEE软件对象

在SMI Cluster Manager配置中，识别本地CEE软件包及其SHA-256哈希。

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

使用批准的软件包中的精确SHA-256值。命令中的占位符是故意的，并不代表实际的校验和。

配置集群和运营中心

源配置将群集与SMF运营中心、本地存储库、管理端点和部署设置相关联。站点特定的标识符被替

换为占位符。

```
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
```

参数	示例配置中的含义
ops-centers smf <smf-ops-center-name>	将群集与SMF运营中心实例相关联。
存储库本地	指定部署的应用存储库和版本。
sync-default-repository true	在同步期间使用配置的默认存储库。
netconf-port 2029	指定NETCONF管理连接端口。
ssh-port 2028	指定安全外壳(SSH)管理连接端口。
use-volume-claims true	允许使用针对持久存储要求的卷声明。
自动部署false	禁用自动部署，以使同步和验证保持显式控制。
单节点false	指定不处于单节点模式的部署。



注意：包和存储库标识符是源配置中的示例。在其他集群中使用版本兼容性和终端值之前，请确认这些值。

同步和验证部署

在软件和运营中心配置准备就绪后运行集群同步操作。

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

检查同步状态和日志。

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

确认同步已成功完成，并且已部署预期的CEE Pod和服务。

⚠ 警告：集群同步和软件部署可以更改运行环境。根据批准的维护和部署程序应用更改。

CEE运营中心和运营管理

CEE Ops Center为CEE服务提供操作界面。该工作负载支持集群内CEE功能的用户管理、身份验证、配置和show命令。SMI集群管理器通过管理配置将运营中心与目标部署相关联。

运营中心属于管理平面。Prometheus、Alertmanager、Fluent Bit/fluent-proxy、HEC、syslog和OpenTelemetry属于监控和遥测路径。分离这些职责可简化故障排除。

CEE可观测性架构

CEE可观察性包括指标、警报、日志、CIMC警报和批量统计数据。这些服务是相关的，但数据路径和使用者不同。

功能	主要用途	典型目的地或消费者
指标	从节点、Kubernetes和服务收集并查询时间系列测量值。	普罗米修斯，格拉法纳和塔诺斯。
风险通告	评估警报规则和路由警报事件。	警报管理器、警报路由器、运营中心和外部接收器。
日志	将日志和事件记录转发到外部收集器或后端。	Splunk和其他日志收集器。
CIMC警报	导出思科集成管理控制器警报以进行监控。	CEE指标/警报和Grafana。
批量统计数据	创建定期统计快照。	CSV快照和下游处理或分析。

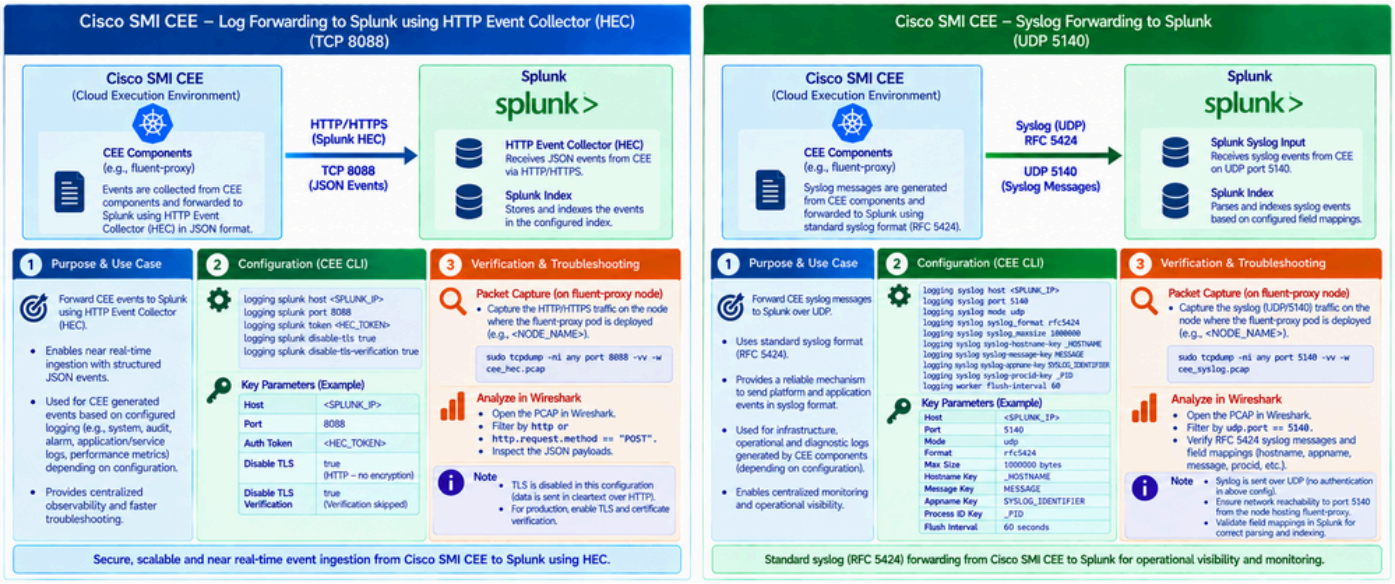
Splunk集成：日志传输架构

源描述两个CEE到Splunk的路径。两者都可以向Splunk传送事件，但它们使用不同的协议和接收接口。

```
CEE
  |-- logging splunk --> HEC / TCP 8088 --> Splunk HEC input
  |
  +-- logging syslog --> RFC 5424 / UDP 5140 --> Splunk syslog input
```

每条路径所承载的事件类型取决于CEE配置和实施的转发管道。两个已配置的接口未确定每个接口都传输互斥的事件类别。

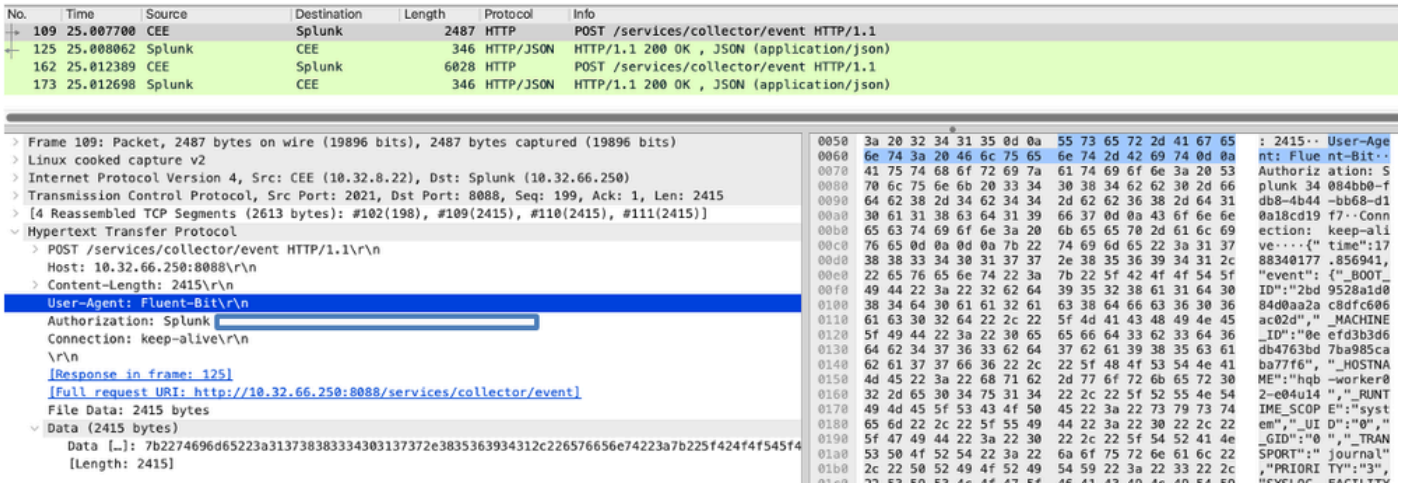
分别跟踪路径。成功的HEC交付不会确认系统日志交付，而成功的系统日志交付不会确认HEC交付。



CEE Splunk与单独的HEC和系统日志转发路径集成

Splunk HTTP事件收集器转发

Splunk HEC接受HTTP事件提交并使用HEC身份验证令牌。CEE将事件直接转发到已配置的HEC服务，而不是为此路径要求基于文件的接收。



CEE到TCP端口8088上的Splunk HTTP事件收集器转发架构

HEC配置模型

原始实验示例包含CEE Splunk端点的这些设置。摘录会记录源行为，并且不是推荐的生产配置。

⚠ 警告：源示例同时禁用TLS和证书验证。这会使遥测和HEC凭证在网络上被拦截。对于生产，请根据支持的CEE版本配置启用TLS和证书验证并保护HEC身份验证令牌。

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

在源体系结构中，CEE日志/事件生成器通过相关的Fluent转发组件转发到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
```

捕获HEC流量并对其进行故障排除

当fluent-proxy传输HEC流量时，在CEE名称空间中识别fluent-proxy pod及其Kubernetes工作节点。

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

在传输HEC流量的Kubernetes节点上，捕获HEC端口的数据包。

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

对于启用TLS的连接，数据包捕获会显示传输建立和目标详细信息，但通常不会显示HTTP负载。如果禁用了TLS，则可以在捕获中看到事件内容和身份验证资料。

⚠ 警告：数据包捕获和日志可以包含敏感的遥测和凭证。限制收集和传输至授权支持工作流程并保护捕获文件。

通过UDP 5140的系统日志转发

第二个Splunk集成路径使用RFC 5424格式和UDP端口5140转发系统日志记录。源配置还定义字段映射、最大消息大小和工作器刷新间隔。

```
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字段映射

CEE源字段	系统日志字段或用途
主机名(_O)	在生成的系统日志记录中标识源主机。
邮件	传送日志消息正文。
系统日志标识符	提供系统日志应用程序或程序标识符。
_PID	携带源进程标识符。

UDP传输和数据包捕获

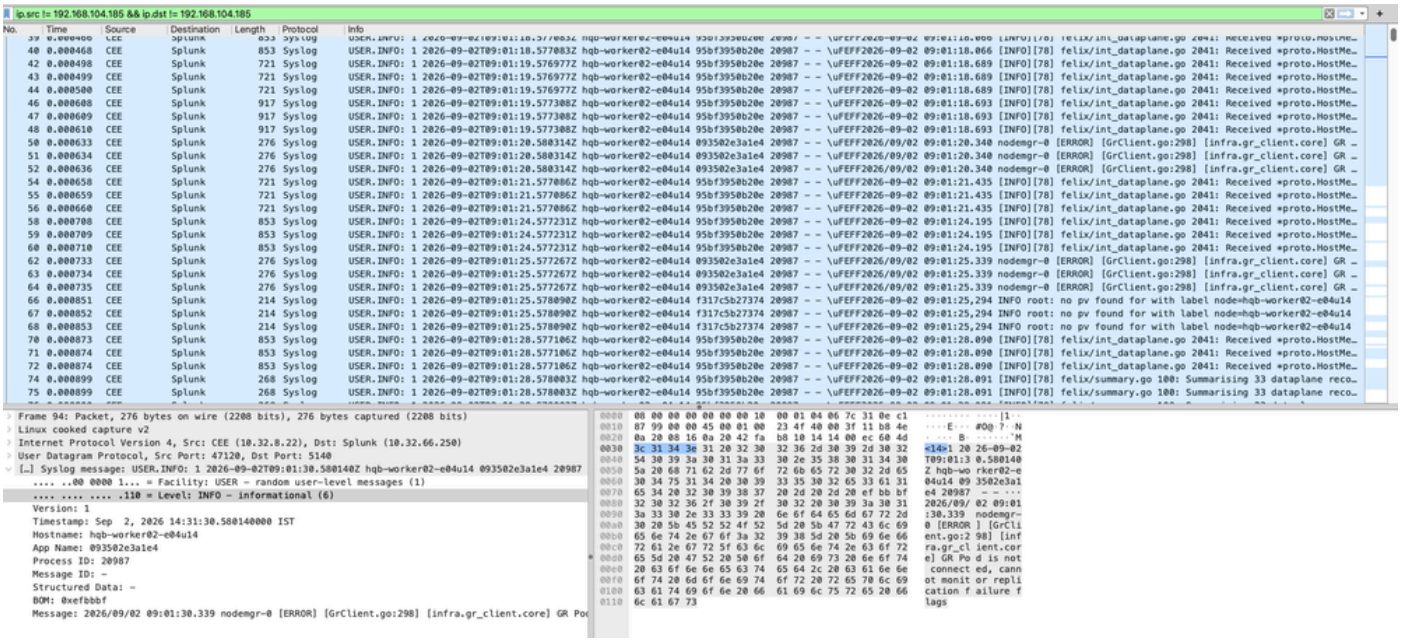
UDP是无连接协议，既不提供传输传输确认，也不提供重新传输。故障排除必须考虑数据包丢失、路由、最大传输单位(MTU)、分段、接收方可用性和队列/速率行为。

在传送系统日志流量的接口或Kubernetes节点上，运行：

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

如果fluent-proxy转发系统日志流量，则托管该组件的节点是适当的数据包捕获点。在收集数据包之前检验转发路径。

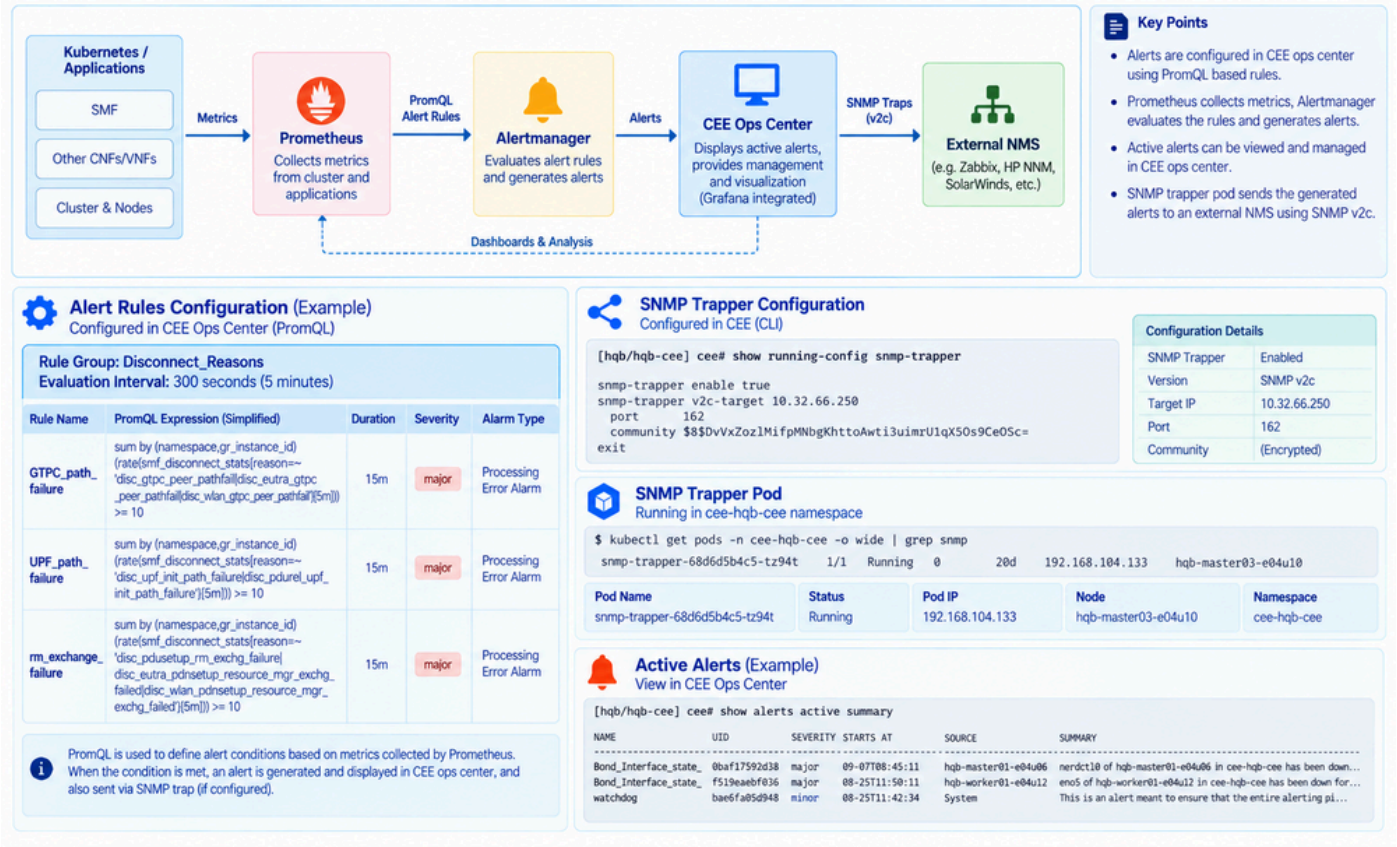
注意：RFC 5424定义独立于所选传输的系统日志消息格式。源方案使用UDP 5140。基于TLS的系统日志传输是另一个选项，它需要兼容的发送方和接收方配置。



使用UDP端口5140和RFC 5424字段将CEE系统日志转发到Splunk

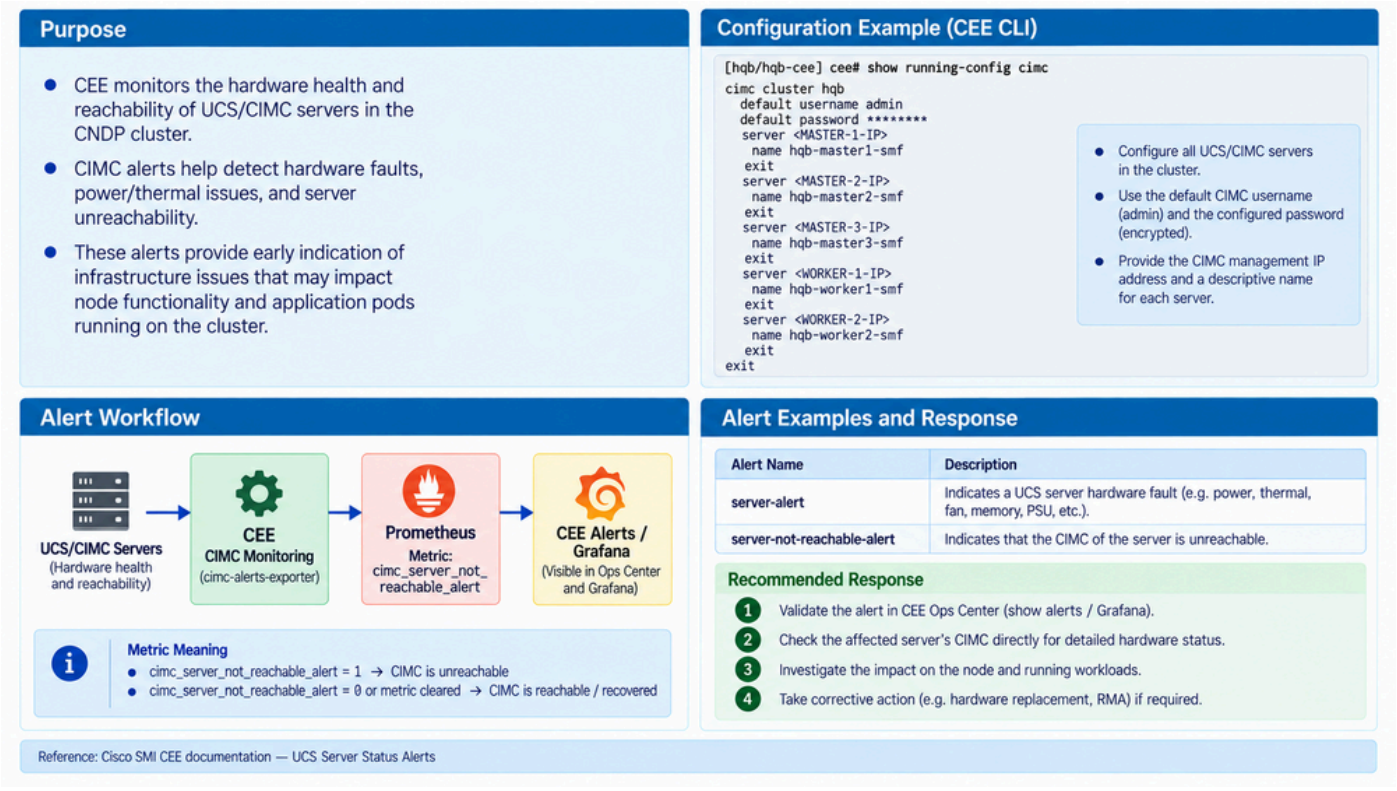
警报、SNMP和CIMC可观察性

CEE警报使用Prometheus和Alertmanager。Prometheus评估指标和警报规则。Alertmanager将警报事件路由到接收器，并且警报路由器提供额外的路由支持。CEE警报记录器提供历史警报记录，以便通过CEE运营中心进行检索。



CEE Prometheus和Alertmanager警报转发和SNMP架构

CIMC警报集成提供相关的基础设施监控路径。cimc-alerts-exporter收集CIMC警报信息并公开该信息，以便在Grafana中进行监控和可视化。



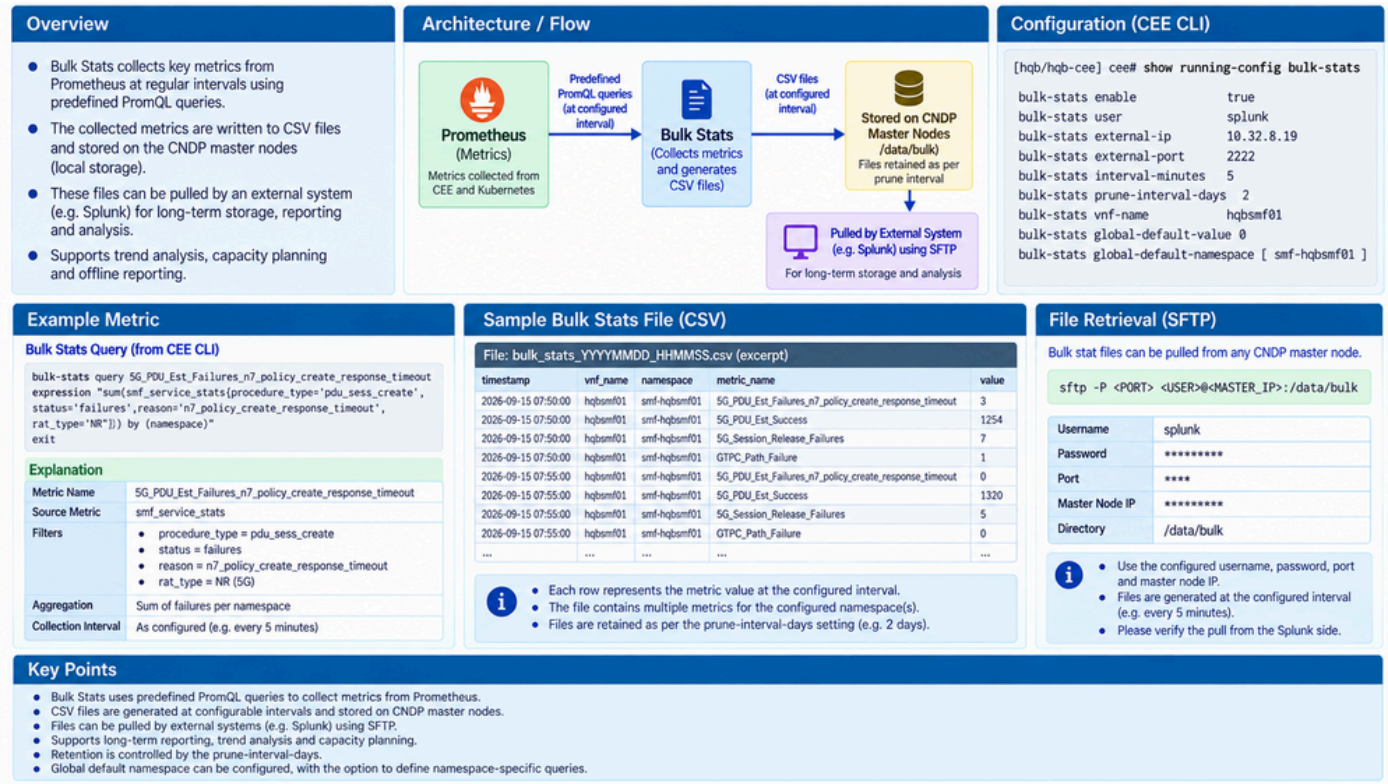
CEE CIMC警报导出器与监控控制面板集成

SNMP集成是一个告警和管理接口；它不能与Splunk HEC或系统日志转发互换。协议和事件传送路径保持不同。

相关管理信息库(MIB)参考包括CISCO-CNEE-MIB.my和CISCO-SMI.my。

批量统计数据

CEE bulk-stats服务创建通过Prometheus收集的统计信息的定期逗号分隔值(CSV)快照。这些是统计快照，而不是应用日志记录流。



CEE批量统计数据服务根据Prometheus指标创建定期CSV快照

Bulk-statistics输出支持周期性报告、趋势分析和下游数据处理。仅当部署明确将CSV/统计信息数据转发或导入Splunk时，才将其包括在Splunk集成路径中。

OpenTelemetry系统网关

较新的Cisco SMI版本支持平台管理的OpenTelemetry收集器网关。网关通过OpenTelemetry Protocol(OTLP)从应用接收遥测，并将支持的指标和日志转发到本地或远程后端。

注意：Cisco SMI Cluster Manager Operations文档确定了与版本2026.03.1的OpenTelemetry网关集成。在源示例描述的特定部署中未验证网关，因此本节介绍发布的配置模型，而不是验证该环境中的操作。

系统网关型号

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

网关配置概念

启用OpenTelemetry Collector网关并选择本地指标和日志后端。

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

当部署需要外部服务暴露时，配置可以包括外部IP。

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

为网关导出器配置可选代理设置。

```
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
```

本地后端选项控制平台托管系统网关如何将遥测发送到内置后端。外部IP暴露和代理设置取决于拓扑和安全要求。

远程导出器

导出器	信号	技术用途
otlp	日志，度量	将遥测发送到接受OTLP over gRPC的后端。
otlphttp	日志，度量	将遥测发送到接受HTTP OTLP的后端。
splunkhec	日志	将日志发送到Splunk HEC终端。
日记簿	日志	将日志写入支持的节点日志。
调试	日志，度量	支持受控验证和故障排除。

OpenTelemetry管道遵循接收、处理和导出模式。接收方接收遥感勘测；处理器过滤或转换数据；导出器将所选信号传送到远程或本地后端。

源还区分代理行为：otlp使用收集器实例代理设置，而otlphttp和splunkhec支持导出器级代理覆盖，其中部署的版本公开了该配置。

请比较OpenShift OpenTelemetry

Cisco CEE和OpenShift具有共同的架构模式：openTelemetry Collector可以位于仪表式应用和可观察性后端之间。它们的管理和安装模式不同。

概念	CEE OpenTelemetry系统网关	OpenShift OpenTelemetry模式
遥测源	OpenTelemetry-enabled CEE和应用工作负载	支持OpenTelemetry的OpenShift工作负载
协议	OTLP	OTLP
收集器角色	平台管理的系统网关	OpenTelemetry Collector部署或实例
渠道概念	接收、处理、导出	接收、处理、导出
后端灵活性	本地后端和支持的远程导出器	导出器驱动后端集成
Splunk集成	文档化的CEE配置中的splunkhec导出器	Splunk HEC导出器（配置时）

这种比较是架构性的。这两个平台并未宣称以相同方式实施OpenTelemetry。OpenShift通常使用OpenTelemetry Operator/Collector部署模式，而Cisco SMI系统网关是平台管理的。

源中讨论的OpenShift参考架构显示收集器从Kubernetes工作负载向Splunk over HEC转发遥感勘测。它说明的是基于收集器的模型，而不是用于示例CEE安装的经验证的集成。

检查配置

验证CEE同步

检查SMI Cluster Manager同步状态和日志，并确认已部署预期的CEE工作负载。

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

分别验证HEC和系统日志

确认HEC路径将事件发送到已配置的TCP 8088终端，并且Splunk收到这些事件。分别确认系统日志路径将UDP 5140记录发送到配置的侦听程序。

使用相应部分中的数据包捕获方法，并将数据包时间戳与已配置的收集器上收到的事件相关联。

检验可观察服务

确认指标、警报路由、CIMC警报和批量统计数据快照是否按照针对已安装版本设计的方式运行。如果启用了OpenTelemetry，请使用支持的SMI Cluster Manager操作过程验证接收器、管道和导出器运行状况。

预期行为

组件或路径	预期结果
SMI集群管理器	集群同步完成，并且部署所需的CEE服务。
运营中心	授权用户可以访问操作功能和支持的配置/监控命令。
Splunk HEC	事件流量到达TCP端口8088上配置的HEC侦听程序。
系统日志	RFC 5424格式的事件到达配置的UDP端口5140侦听程序。
警报和CIMC	Alertmanager和相关导出器显示已配置的警报信息。
批量统计数据	根据收集的统计数据生成定期CSV快照。
OpenTeletry	在配置了网关的受支持版本中，OTLP信号流经选定的后端/导出器管道。

决策流程

观察	下一个检查
同步后缺少CEE服务。	检查Cluster Manager同步状态、日志、软件项目和Ops Center参数。
缺少HEC事件。	识别转发Pod/节点，验证TCP 8088流量、HEC目标、身份验证和TLS配置。
缺少系统日志事件。	验证UDP 5140目标、RFC 5424格式、数据包流和接收器行为。

观察	下一个检查
缺少警报或CIMC数据。	检查Prometheus/Alertmanager路由、alert-router和cimc-alerts-exporter操作。
缺少批量统计数据。	确认批量统计数据服务操作、Prometheus数据可用性和CSV快照生成。
缺少OpenTelemetry导出。	验证对已安装版本、网关配置、接收器和导出器状态以及管道成员资格的功能支持。

结论

CEE是一个基于Kubernetes的分层执行和可观测性环境，它围绕SMF应用。Kubernetes命名空间分离将平台操作、CEE服务和应用工作负载划分到不同的域。在CEE中，监控、警报、日志记录和批量统计数据是具有独立职责的专门服务。

Splunk的关键区别在于基于TCP 8088的HEC和基于UDP 5140的syslog。这些是具有不同协议、配置和故障排除过程的独立转发路径。较新的OpenTelemetry系统网关添加了基于OTLP的收集器和导出器模型。它与OpenShift OpenTelemetry的相似之处在于架构，并且必须验证特定CEE版本和部署的网关操作。

相关内容

- Cisco CEE配置和管理指南 — 常见执行环境
- Cisco CEE配置和管理指南 — 日志记录命令
- Cisco SMI Cluster Manager操作 — 同步和OpenTelemetry
- RFC 5424 — 系统日志协议

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。